

Welcome to the US Coast Guard Auxiliary **Privacy at DHS** Training.

**Independent Learner Instructions.**

This document is derived from the mandatory training of the same name. It contains both images and narratives regarding the training topic and is provided in a “presenter notes” format.

As an independent learner you are expected to read all content contained in this document to include both the text within the images and the notes below the image (if any). Some images do not have notes or are self-explanatory.

As you work through this training material you should keep in mind that as an independent learner, you are responsible and accountable for learning and understanding the course content.


You should also understand its importance to our organization and the execution of our varied missions and be able to apply the knowledge gained through this independent training experience.





# Privacy at DHS: Protecting Personal Information

Reviewed, DIR-T USCGAUX

In our mission to secure the homeland, we need to collect personal information from citizens, legal residents and visitors, and we are obligated by law and DHS policy to protect this information to prevent identity theft or other adverse consequences of a privacy incident or misuse of data. This brief course is designed to raise your awareness of the importance of maintaining privacy in the workplace, and will convey methods of safeguarding personal information



# Introduction



- Hi, I'm the DHS Privacy Man. For the next 15 to 20 minutes, I want to talk to you about the importance of safeguarding personal information, such as Social Security numbers, that DHS may collect or store in its databases or in paper files. Congress and OMB have mandated privacy training for both employees and contractors at all federal agencies to help staff identify and mitigate privacy risks related to sensitive personal information, which I will define in a moment.

Reviewed, DIR-T USCGAUX

This course addresses the standards that the Department of Homeland Security (DHS) has adopted to safeguard personal information. This is similar to the HIPPA regulations that govern the security of personal information in the healthcare industry and FERPA that does the same job in education. Remember, this is about more than just the information of Auxiliarists; it can include our gold side shipmates, others in federal service, and members of the public we are working to help recover after an incident.



## Objectives

- In our mission to secure the homeland, DHS needs to collect personal information, also known as Personally Identifiable Information or PII, from citizens, legal residents, and visitors, and we are obligated by law and DHS policy to protect this information to prevent identity theft or other adverse consequences of a privacy incident or misuse of data. As DHS staff who might collect, use, or share PII, you need to:
- Know how to protect PII; and
- Report any suspected or confirmed privacy incidents.



Reviewed, DIR-T USCGAUX

As an Auxiliarist you may have access to Personally Identifiable Information (PII) from a variety of sources, including official Auxiliary documents, copies of vessel inspection forms, registration for public education events, information about members of the public who have been involved in an incident, and many other sources. All of these sources of information need to be properly managed and protected to safeguard the trust that our shipmates and the public have placed in us.



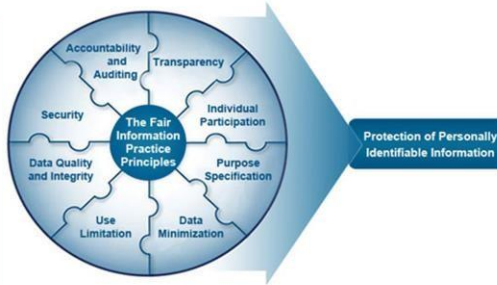
## Privacy is Embedded into Our Mission

If you are a program manager or system owner, it is important to understand your responsibilities for completing privacy compliance documentation before your system becomes operational.

Depending on the nature of your system or program, privacy compliance documentation such as a Privacy Impact Assessment, required by the E-Government Act of 2002, and/or a System of Records Notice, required by the Privacy Act of 1974, may be required.


Although this course will not get into the details of how to prepare these documents, it is important to recognize that privacy compliance gaps can put your system or program at risk. For example, a recent Government Accountability Office report recommended that the Chief Privacy Officer investigate whether a system should be suspended until privacy compliance documentation could be completed.

We encourage program managers and system owners to consult with their Component Privacy Officer or Privacy Point of Contact early in the Systems Development Lifecycle to ensure that privacy requirements are addressed.




Reviewed, DIR-T USCGAUX

While as an Auxiliarist you may not be a program owner it is important to understand how privacy compliance is managed in DHS. We all have a responsibility to properly manage PII and part of that is understanding the system in which we work.



# What is Personally Identifiable Information?


Caution: Handle with Care



Name, Email, and Home Address

Sensitive PII

Caution: Handle with Care



Driver's License Numbers


Sensitive PII

- DHS defines personally identifiable information or PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
- The graphic to the left shows some examples of PII.


Reviewed, DIR-T USCGAUX

DHS defines personally identifiable information or PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

**Sensitive PII** includes but is not limited to the information pictured here, which includes Social Security numbers, driver's license numbers, Alien Registration numbers, financial or medical records, biometrics or a criminal history. This data requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.



# What is Personally Identifiable Information?



- So what do I mean when I refer to personal information?
- At DHS we call personal information “personally identifiable information”, or PII:
- DHS defines **PII** as *any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.*

Reviewed, DIR-T USCGAUX

PII and Sensitive PII as privacy incidents are not necessarily cut and dried. In some cases, PII that is not Sensitive would be reported as a privacy incident depending on context. For example, a loss of a contact list with the names of people who attended training would not be considered a privacy incident. However, if it is a list of employees who are being disciplined for not attending training and it is lost or compromised, then that would be considered a privacy incident. In this instance, it is the context of the information that would cause this to be a reportable privacy incident.



# What is Personally Identifiable Information?

Caution: Handle with Care



Passport Numbers

Sensitive PII



- Also, the loss of Sensitive PII even in an encrypted or password-protected format could become a privacy incident. For instance, if encrypted or password-protected Sensitive PII, along with the "key" or password to access the information, is sent to a person without a "need to know" or to a personal e-mail address, this would be considered a privacy incident.
- If you're confused, stay with me and in a few minutes I will walk you through specific examples on how you can safeguard Sensitive PII.

Reviewed, DIR-T USCGAUX

Also, the loss of Sensitive PII even in an encrypted or password-protected format could become a privacy incident. For instance, if encrypted or password-protected Sensitive PII, along with the "key" or password to access the information, is sent to a person without a "need to know" or to a personal e-mail address, this would be considered a privacy incident.

If you're confused, stay with me and in a few minutes I will walk you through specific examples on how you can safeguard Sensitive PII.



## Examples of PII Collection at DHS

- DHS Components collect a wide range of PII for reasons varying from national security to the distribution of disaster relief funds.
- To give you a sense of the magnitude of the PII handled by DHS, every day we collect and safeguard PII on over 3 million domestic and international travelers. And that's just one example.

DHS Component	Collects PII about:
Chief Human Capital Office	Employees
Federal Emergency Management Agency	Disaster Victims
Customs and Border Protection, Transportation Security Administration, and US-VISIT	Travelers
Immigration and Customs Enforcement	Criminal investigations and immigration enforcement
U.S. Citizenship and Immigration Services	Asylum seekers and residents
National Protection and Programs Directorate	Critical infrastructure protection

Reviewed, DIR-T USCGAUX

How do you collect or use PII as an Auxiliarist? Do you work in Auxdata or manage communications for your flotilla where you access information on your shipmates? Do you serve as a vessel inspector and retain copies of inspection forms that include information about vessel owners? Do you work events as part of public relations and collect contact information from members of the public who may be interested in taking a class or joining the Auxiliary? All of these tasks and many more that we conduct as Auxiliarists creates PII for which we as individuals and an organization are responsible.



## Potential Consequences of Not Protecting PII

- **For DHS:**
  - Loss of public trust
  - Increased Congressional oversight
  - Loss of funding
- **For the victim:**
  - Identity theft
  - Loss of benefits
  - Embarrassment
- **For the person causing the privacy incident:**
  - Counseling and training
  - Loss of employment
  - Civil & criminal penalties



Reviewed, DIR-T USCGAUX

If we fail to protect PII, there can be severe consequences for everyone. Most privacy incidents occur when employees mishandle PII due to a lack of awareness of PII safeguards, and when that occurs, they receive counseling and additional training.

But we have also experienced intentional privacy incidents at DHS. For example, a FEMA employee was sentenced to 5 years in prison for stealing the identities of more than 200 disaster victims who had applied for government assistance.




## Report Privacy Incidents

- If you:
  - Lose, allow, or witness unauthorized access to Sensitive PII.
  - Unintentionally release Sensitive PII.
  - Misuse Sensitive PII.
  - Cause files or systems to become compromised.
  - Know or suspect that any of the above has occurred.
- You **MUST** report the privacy incident, either suspected or confirmed, **immediately** to your supervisor, Component help desk, privacy officer, or privacy point of contact.




Reviewed, DIR-T USCGAUX

Sometimes what appears to be a completely innocent event can compromise PII. Forgetting a clipboard with vessel inspection records when you're at a marina, leaving a flotilla folder behind at a coffee shop, or accidentally attaching the incorrect file to an e-mail are all examples of ways we can accidentally cause a privacy incident as Auxiliarists. Even if you think it is minor and nothing will happen you need to report every incident. Reporting the incident isn't to get anybody in trouble, it's the right thing to do to fulfill our duty to safeguard the PII with which we've been entrusted.



## A Day in the Life of PII



- The following scenario is based on the most common types of privacy incidents at DHS. In this scenario, you will play the role of a FEMA employee who processes disaster assistance claims that contain Sensitive PII.
- Please note that the privacy protection best practices cited here may not reflect the current privacy policies in every DHS component.
- Review the 2 Job Aids: Handbook for Safeguarding PII At DHS, and How to Safeguard PII. Consult them throughout the scenario to make sure you use the proper safe handling procedures and avoid privacy incidents as you access, use and share Sensitive PII.

Reviewed, DIR-T USCGAUX

The following scenario is based on the most common types of privacy incidents at DHS. In this scenario, you will play the role of a FEMA employee who processes disaster assistance claims that contain Sensitive PII.

Please note that the privacy protection best practices cited here may not reflect the current privacy policies in every DHS component.

Open the two Job Aids by clicking on the Resources folder in the progress bar above, and consult them throughout the scenario to make sure you use the proper safe handling procedures and avoid privacy incidents as you access, use and share Sensitive PII.

To increase your awareness of the proper procedures for collecting, using, sharing and disposing of Sensitive PII, we've created two job aids. The first is called How to Safeguard PII, and is a summary of the Handbook for Safeguarding Sensitive PII at DHS. The second job aid is called Telework Best Practices, and outlines the proper protocol for handling Sensitive PII while teleworking.

In this scenario, you will play the role of a FEMA employee who processes disaster assistance claims that contain Sensitive PII. Consult the two job aids throughout the scenario to answer the questions correctly.



## A Day in the Life of PII

- To increase your awareness of the proper procedures for collecting, using, sharing and disposing of Sensitive PII, we've created two job aids. The first is called How to Safeguard PII, and is a summary of the Handbook for Safeguarding Sensitive PII at DHS (also available in the Resources folder). The second job aid is called Telework Best Practices, and outlines the proper protocol for handling Sensitive PII while teleworking.
- In this scenario, you will play the role of a FEMA employee who processes disaster assistance claims that contain Sensitive PII. Consult the two job aids throughout the scenario to answer the questions correctly.

Reviewed, DIR-T USCGAUX



## A Day in the Life of PII – 2

### Collecting and Accessing Sensitive PII

- Privacy Man: You've just finished taking a much deserved break and have returned to your workstation. It seems like you've been processing disaster assistance claims for months, when in reality it's only been three long days since the record-breaking flood hit the northeast.
- Katelyn Baker: Hello, you don't know me, but I am helping distribute disaster relief funds. Can you give me Polly Smith's Social Security number?



Reviewed, DIR-T USCGAUX

This is a scenario that you may encounter while working at a DHS facility:

You've just finished taking a much deserved break and have returned to your workstation. It seems like you've been processing disaster assistance claims for months, when in reality it's only been three long days since the record-breaking flood hit the northeast. After you unlock your computer and continue working, someone approaches the entrance to your cube...

Katelyn Baker: Hello, you don't know me, but I am helping distribute disaster relief funds. Can you give me Polly Smith's Social Security number?



## PII Self-Check Question 1

- Q: In this case, what is the proper procedure for sharing Polly Smith's Sensitive PII?
- A) Ask the employee for her identification and her reason for requesting Miss Smith's Sensitive PII.
- B) Provide the employee with the information she requested.
- C) Contact your supervisor immediately and let her know someone you've never met before is requesting Sensitive PII.
- D) Tell the employee you will email it to her after you finish the claim you are working on.

Reviewed, DIR-T USCGAUX



## PII Self-Check Answer 1:

- Q: In this case, what is the proper procedure for sharing Polly Smith's Sensitive PII?
- **A) Ask the employee for her identification and her reason for requesting Miss Smith's Sensitive PII.**
- B) Provide the employee with the information she requested.
- C) Contact your supervisor immediately and let her know someone you've never met before is requesting Sensitive PII.
- D) Tell the employee you will email it to her after you finish the claim you are working on.

Reviewed, DIR-T USCGAUX

Feedback for answer A:

**You chose option A. That's right!** The proper procedure is to ask the requestor for her identification and her reason for requesting the PII. Access to PII must meet two requirements: (1) the requestor must have a need to know the information in their official capacity; and (2) if they are a non-DHS employee or contractor, the disclosure of PII must be authorized and in compliance with the Privacy Act of 1974. Please consult your Component legal counsel before disclosing any PII to persons who are not agency employees.

Feedback for Answer B:

**You chose option B. Try again.** Providing Sensitive PII to a person you don't know without knowing the reason they need the Sensitive PII is a privacy incident waiting to happen. Please remember to reference the job aid.

Feedback for Answer C:

**You chose option C. That is incorrect.** Remember, you don't know this person or why they need the Sensitive PII, but her request could be legitimate. Instead of immediately involving your supervisor, the proper procedure is to ask the employee for her identification and her reason for requesting the Sensitive PII. Access to Sensitive PII is based upon a person having a "need to know", i.e., when the information relates to their official duties. So, if you are ever in doubt as to the person's "need to know," you should consult your supervisor and get back to the



person requesting the Sensitive PII.

Feedback for answer D:

**You chose option D. Try again.** Providing Sensitive PII to a person you don't know without knowing the reason they need the Sensitive PII is a privacy incident waiting to happen. Please remember to consult the job aid.



## A Day in the Life of PII – 3

### Collecting and Accessing Sensitive PII

- Privacy Man: You let the employee know that her ID badge was turned backwards, asked her to introduce herself and why she needs to know Miss Smith's Sensitive PII.
- Katelyn Baker: Oh, I'm sorry. My name is Katelyn Baker and I'm a contractor assigned to assist with the distribution of disaster relief funds. Polly Smith hasn't received her assistance funds yet. I need her Social Security number so I can check on the payout of her funds.
- Privacy Man: You recognize Katelyn's name and heard that she and her employer have been doing a great job helping FEMA respond to the numerous claims that have been filed. You let Katelyn know that you are currently busy with another request, but will email her Polly Smith's SSN later today.
- Later that afternoon, you begin drafting the email to Katelyn when you remember that she is an outside contractor. You know that many privacy incidents are the result of poor email practices, so you need to send this Sensitive PII using the proper procedure.



Reviewed, DIR-T USCGAUX

One of the important things to remember when you're dealing with PII is that it's OK to ask questions. Nobody should be offended or upset when you take the time to ensure that you're following procedure and safeguarding the PII with which you've been entrusted. Privacy is everybody's job.



## PII Self-Check Question 2

- Q: What is the proper method for emailing Sensitive PII outside of the Department?
- A) Sensitive PII should not be sent outside of the Department via email.
- B) Type the requested Sensitive PII into the body of the email and send the email.  
Follow-up with a phone call to the recipient to make sure they received the information.
- C) Save the Sensitive PII in a protectable file type, encrypt or password-protect the document, attach it to the email, and then follow up with either a phone call or a separate email containing the password to open the file.

Reviewed, DIR-T USCGAUX



## PII Self-Check Answer 2

- Q: What is the proper method for emailing Sensitive PII outside of the Department?
- A) Sensitive PII should not be sent outside of the Department via email.
- B) Type the requested Sensitive PII into the body of the email and send the email.  
Follow-up with a phone call to the recipient to make sure they received the information.
- **C) Save the Sensitive PII in a protectable file type, encrypt or password-protect the document, attach it to the email, and then follow up with either a phone call or a separate email containing the password to open the file.**

Reviewed, DIR-T USCGAUX

Feedback for answer A:

**You chose option A. Try again.** Sending Sensitive PII outside of the Department is okay as long as you follow the proper procedure. Remember to reference the Job Aid.

Feedback for answer B:

**You chose option B. That is incorrect.**

Sending Sensitive PII in the body of an email to an external party is a privacy incident. The proper procedure is to:

1. Save the Sensitive PII in a Word, Excel or other protectable file type.
2. Encrypt and/or password-protect the document using WinZip or Adobe Acrobat until the Department implements PKI encryption. [Be sure to consult the Handbook for Safeguarding Sensitive PII in the Resources folder for specific instructions on how to encrypt or password protect a file.]
3. Attach it to the email.
4. Make sure you have selected the correct recipient and do not hit "reply all" unless everyone on the email list has a "need to know."
5. Send the encrypted/password-protected document as an email attachment.
6. Provide the password to the recipient by phone or in a separate email.

It's important to note that some DHS components require email encryption or password protection for internal as well as external sharing of Sensitive PII.

Feedback for answer C:

**You chose option C. That's right!** Be sure to consult the Handbook for Safeguarding Sensitive PII in the Resources folder for specific instructions on how to encrypt or password protect a file.

It's important to note that some DHS components require email encryption or password protection for internal as well as external sharing of Sensitive PII.



# A Day in the Life of PII – 4

## Collecting and Accessing Sensitive PII

- Privacy Man: After sending the email, you called Katelyn Baker to provide her with the password to access the files you just sent.
- Katelyn Baker: Thank you so much for emailing me Miss Smith's information. The password works and I'm looking at her information now. While I have you on the phone, can I ask you to email me copies of the claim forms for the 20 claimants on Canal Street that we discussed? Sorry, but I forgot to ask you when I stopped by.
- Privacy Man: You tried to email the 20 claim forms to Katelyn, but the files are too large to send via email. Your only other option is to mail the Sensitive PII to her. You know that mail often gets compromised while in transit, so it's a shame that you are not able to email the forms or else you could scan them and send password-protected versions to her.



Reviewed, DIR-T USCGAUX

Sometimes taking the right steps to ensure the security of PII means that things move more slowly than they would otherwise. This is OK; it's much better to follow procedure and ensure that PII is safe than to speed things up at the expense of security. Just one failure to secure PII can result in major consequences.



## PII Self-Check Question 3

- Q: Since you can't email the claim forms to Katelyn's office, what is the preferred method for mailing Sensitive PII externally?
- A) Scan the claim forms and save the data onto an encrypted CD or USB flash drive. Seal it in an opaque envelope and mail it using First Class or Priority Mail, a courier, or a traceable commercial delivery service like UPS, the USPS, or FedEx.
- B) Mail a hard copy of the claim forms using a traceable commercial delivery service like UPS, the USPS, or FedEx.

Reviewed, DIR-T USCGAUX



## PII Self-Check Answer 3

- Q: Since you can't email the claim forms to Katelyn's office, what is the preferred method for mailing Sensitive PII externally?
- **A) Scan the claim forms and save the data onto an encrypted CD or USB flash drive. Seal it in an opaque envelope and mail it using First Class or Priority Mail, a courier, or a traceable commercial delivery service like UPS, the USPS, or FedEx.**
- B) Mail a hard copy of the claim forms using a traceable commercial delivery service like UPS, the USPS, or FedEx.

Reviewed, DIR-T USCGAUX

Feedback for answer A:

**You chose option A. That's right!** You really want to avoid mailing anything that contains Sensitive PII, but if you have to, the preferred method is to:

1. Scan the hard copy Sensitive PII and save it onto an encrypted CD, USB flash drive, or other DHS-approved portable media.
2. Mail the portable media using First Class or Priority Mail, a courier, or a traceable commercial delivery service like UPS, the USPS, or FedEx.

Feedback for answer B:

**You chose option B. Try again.** Mailing hard copies of the claim forms using a traceable commercial delivery service like UPS, the USPS, or FedEx does not properly safeguard the Sensitive PII being sent. Remember to reference the Job Aid for the preferred method for mailing hard copy Sensitive PII.





## A Day in the Life of PII – 5

### Sending Sensitive PII Outside of DHS

- **Privacy Man:** You get a phone call from one of your fraud investigators requesting Ms. Smith's claim file. He wants to give it one of his law enforcement contacts at the local Police Department. You should know that the Privacy Act prohibits disclosing personal information outside the agency without written permission from Ms. Smith, unless an exception applies.
- What should you do? To answer the scenario, review the Handbook for Safeguarding Sensitive PII at DHS and go to page 8, Minimize Proliferation of Sensitive PII.



Reviewed, DIR-T USCGAUX



## A Day in the Life of PII – 6

### Accessing and Using Sensitive PII While Away from the Office

- You've completed Katelyn's request for PII and now it's 5 o'clock and time to head home.
- But first, since you are working from home tomorrow, you need to pack your briefcase with everything you need, including some Sensitive PII.



Reviewed, DIR-T USCGAUX

This is a scenario that is especially important for Auxiliarists. Because few of us have permanent bases and offices from which to conduct Auxiliary business we are in the position of transporting PII and keeping it at home. It is important that we consider the best way to keep that information safe when we're working from home and meeting and conducting Auxiliary business in other locations.



## PII Self-Check Question 4

- Q: What is the best way to access Sensitive PII while away from the office?
- A) Email the Sensitive PII, via a password-protected document, to your personal email account that you can access from home.
- B) Pack hard copies of the Sensitive PII into your briefcase in a folder marked "Confidential."
- C) Save Sensitive PII to or access it from an encrypted, DHS-approved portable electronic device such as a laptop, Blackberry, CD, or other removable media.

Reviewed, DIR-T USCGAUX



## PII Self-Check Answer 4

- Q: What is the best way to access Sensitive PII while away from the office?
- A) Email the Sensitive PII, via a password-protected document, to your personal email account that you can access from home.
- B) Pack hard copies of the Sensitive PII into your briefcase in a folder marked "Confidential."
- **C) Save Sensitive PII to or access it from an encrypted, DHS-approved portable electronic device such as a laptop, Blackberry, CD, or other removable media.**

Reviewed, DIR-T USCGAUX

Feedback for answer A:

**You chose option A. Try again.** Sensitive PII should NEVER be sent to a personal email account because it will become susceptible to compromise once it's outside of the DHS firewall. This constitutes a privacy incident. Remember to consult the Job Aid.

Feedback for answer B:

**You chose option B. That is incorrect.** Unless you are authorized to do so, you should never remove **hard copies** of documents containing Sensitive PII from your office. Check with your supervisor or with your component telework policy to see if this is permitted.

If you telework or travel for work, you need to follow these guidelines to safeguard Sensitive PII:

Use DHS-approved portable electronic devices, which are encrypted.

Get your supervisor's permission to remove hard copy Sensitive PII from the office.

Secure all Sensitive PII when not in use.

Log in through the DHS secured portal.

Take advantage of collaboration tools such as SharePoint.

Feedback for answer C:

**You chose option C. That's right!** If you telework or travel for work, you need to follow these guidelines to safeguard Sensitive PII:

Use DHS-approved portable electronic devices, which are encrypted.  
Get your supervisor's permission to remove hard copy Sensitive PII from the office.  
Secure all Sensitive PII when not in use.



## A Day in the Life of PII

### Safeguarding Sensitive PII Summary

- So you've just learned how to prevent the 4 most common privacy incidents at DHS. Allow me to reiterate the key points for you to remember, and highlight some new points:
  - **Sharing Sensitive PII:** It is important to protect Sensitive PII at all times. Share it only with people who have an official "need to know."
  - **Emailing to the wrong recipient or personal accounts:** Never email Sensitive PII to a personal email account. If you need to work on Sensitive PII off site, use a DHS-approved portable electronic device.
  - **Preventing Compromised Mail:** If documents can't be scanned and encrypted or password-protected, mail them in an opaque envelope or container using First Class, Priority Mail, or a traceable commercial delivery service like UPS, the USPS, or FedEx.

Reviewed, DIR-T USCGAUX

Many of the ways we can protect PII are simple, we just need to get in the habit of using good practices. Whenever you're handling PII in the Auxiliary think about what you can do to ensure its security while in your possession. All of us are responsible for protecting PII in all of our roles in the Auxiliary.



## A Day in the Life of PII

### Safeguarding Sensitive PII Summary

- **Accessing Sensitive PII while away from the office.** The best method is to save the Sensitive PII on an encrypted, DHS-approved portable electronic device such as a laptop, Blackberry, CD, USB flash drive, or other removable media.
- **Lost Media:** Do not leave any portable electronic devices in a car. If it is stolen or lost, report it as a lost asset following your component reporting procedures.
- **Lost Hard Copies:** Secure Sensitive PII in a locked desk drawer or file cabinet. When using Sensitive PII, keep it in an area where access is controlled and limited to persons with an official "need to know". Avoid faxing Sensitive PII, if at all possible.
- **Posting Sensitive PII to websites and shared drives:** Do not post Sensitive PII on the DHS intranet, the Internet (including social networking sites), shared drives, or multi-access calendars that can be accessed by individuals who do not have an official "need to know."

Reviewed, DIR-T USCGAUX

Many of the ways we can protect PII are simple, we just need to get in the habit of using good practices. Whenever you're handling PII in the Auxiliary think about what you can do to ensure its security while in your possession. All of us are responsible for protecting PII in all of our roles in the Auxiliary.



## You Can Promote Privacy at DHS

- To promote privacy at DHS, it is important to:
  1. Partner with your Component Privacy Office when planning new or updating existing programs, systems, technologies or rule-makings to ensure compliance with privacy laws.
  2. Follow the procedures outlined in the *Handbook for Safeguarding Sensitive PII* at DHS.
  3. Report all **suspected or confirmed** privacy incidents immediately.
- And when you work with Sensitive PII, be sure to consult the two Job Aids as well as the other resources listed on the Privacy Resources page.



Reviewed, DIR-T USCGAUX

Remember, it's always OK to ask questions and have discussions with your shipmates and partners from other agencies to ensure that PII is being protected. If you are ever in doubt about how PII is being handled use the Chain of Leadership and ask the question. When individual Auxiliarists pay attention to PII and help others recognize the importance of security everybody benefits.





## Privacy Resources

- There are several resources you can reference when handling PII to make sure you are following the proper procedures.
  - Privacy Office website: [www.dhs.gov/privacy](http://www.dhs.gov/privacy)
  - For privacy concerns, consult your Component's Privacy Officer or Privacy Point of Contact.
  - *Handbook for Safeguarding Sensitive PII*
  - How to Safeguard PII Job Aid
  - Controlling Access to a Network Shared Drive Folder.
  - Telework Best Practices Job Aid.



Reviewed, DIR-T USCGAUX



## Completed Training Attestation

### Coast Guard Core Values

- **Honor**
  - Integrity is our standard. We demonstrate uncompromising ethical conduct and moral behavior in all of our actions. We are loyal and accountable to the public trust.”
- **Respect**
  - We value our diverse workforce. We treat each other with fairness, dignity, and compassion. We encourage creativity through empowerment. We work as a team
- **Devotion to Duty**
  - We are professionals, military and civilian, who seek responsibility, accept accountability, and are committed to the successful achievement of our organizational goals. We exist to serve. We serve with pride.

Reviewed: DIR-T USCGAUX

The mandatory training that you have just completed reflects the **Core Values of the U.S. Coast Guard** and **Coast Guard Auxiliary**. As a member of this organization, you have taken an oath to uphold those Core Values. In order to receive completion credit for this training, please read, understand, and sign this document. Once completed, keep a copy for your records and provide a copy to your Flotilla Staff Officer for Information Services (FSO-IS) for AUXDATA entry.

In regards to the selected mandated training modules: Codes: \_\_\_\_\_

I, \_\_\_\_\_ (print name) as a member of District \_\_\_\_\_

Division \_\_\_\_\_ Flotilla \_\_\_\_\_ attest that I have completed and understand the course contents.

Signature: \_\_\_\_\_, Member ID \_\_\_\_\_

Date: \_\_\_\_\_

Course Code	Course Name	Frequency
502379	Building Resilience and Preventing Suicide	Every 5 years
810030	Security Fundamentals	Every 5 years
810015	Privacy at DHS / Protecting Personal Information	Every 5 years
810000	Sexual Harassment Prevention	Every 5 years
810045	Sexual Assault Prevention and Response	Every 5 years
502319	Civil Rights Awareness	Every 5 years
502306	Ethics 1 / Personal Gifts	1 time only
502290	Influenza Training	1 time only