



Homeland
Security

Handbook for Safeguarding Sensitive Personally Identifiable Information

At The Department of Homeland Security

Updated 10-06-2011



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
January 19, 2011

Dear Colleagues,

I am pleased to share with you this new edition of the DHS Privacy Office's *Handbook for Safeguarding Sensitive PII at DHS*, which applies to every DHS employee, contractor, detailee, and consultant.

The Handbook sets minimum standards for how all personnel should handle Sensitive PII at DHS. Your Component Privacy Officer, Program Office, or System Owner may set additional or more specific rules for handling PII, including Sensitive PII, based on the sensitivity of the information involved. The Privacy Office has issued this new edition to clarify your responsibilities with respect to securing Sensitive PII both when in use and when not in use. You will find expanded guidance on this topic in Section 2.0 below.

The Handbook provides step-by-step guidance on how to identify and protect Sensitive PII:

- In the office or an alternate worksite
- On a portable device, such as blackberry or laptop
- When sent by email, fax, or other electronic transfer
- When sent by mail: external, overseas and inter-office
- When stored on a shared drive
- When you are on official travel

The Handbook also provides simple instructions on:

- Encrypting Sensitive PII
- Securing Sensitive PII when it is not in use
- Disposing of Sensitive PII

This Handbook is intended to help you safeguard Sensitive Personally Identifiable Information (PII) in paper and electronic form during your everyday work activities. By observing these guidelines, you will be doing your part to protect the Sensitive PII of our employees, contractors, and the public, by reducing the risk that a serious data breach will occur at DHS. If you have any questions regarding the Handbook please contact your Component Privacy Officer or privacy@dhs.gov.

Sincerely,

A handwritten signature in black ink that reads "Mary Ellen Callahan".

Mary Ellen Callahan
Chief Privacy Officer
Chief Freedom of Information Act Officer
The Privacy Office
United States Department of Homeland Security

Updates to the Handbook for Safeguarding Sensitive PII

Section	Page	Updates
October 2011 Updates		
1.3 New “law enforcement personnel exception” for Alien numbers		
1.3.2	8	<p>Added this section: <i>When non-DHS staff need to send Alien numbers (A-numbers) to DHS law enforcement personnel, and it is not feasible or consistent with operational needs to do so using encrypted emails, non-DHS staff may send unencrypted A-numbers to DHS law enforcement personnel in order to fulfill their DHS law enforcement and immigration enforcement duties.</i></p> <ul style="list-style-type: none"> • <i>The known location of the alien is the only other PII that may be included in the unencrypted emails sent to DHS law enforcement personnel from non-DHS staff (e.g., DHS contractors who need to send emails originating outside the DHS firewall).</i>
January 2011 Updates		
2.2 Limit Use of Sensitive PII		
2.2.1	9	<p>Added the following bullet: <i>Remember that you must secure Sensitive PII in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.</i></p>
2.3 Minimize Proliferation of Sensitive PII		
2.3.3	10	<p>Added the following bullet: <i>Until you dispose of Sensitive PII, keep it secured in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.</i></p>
2.4 Secure Sensitive PII		
2.4.3	10	<p>Edited the third sentence by adding the underlined words: <i>Paper documents must be under the control of the employee or locked in a <u>secure container</u> <u>when not in use.</u></i></p>
2.4.4	10	<p>Edited the entire section: <i>Physically secure sensitive PII (e.g., in a locked drawer, cupboard cabinet, or desk; in a safe; or in another locked container) when not in use and or <u>not otherwise</u> under the control of a person with a need to know. Sensitive PII may also be stored in a room/area <u>space where that has</u> access control measures <u>are employed that to prevent unauthorized access by members of the public, visitors,</u> or other persons without a need to know, such as (e.g., a locked room <u>or floor, or other space</u> an area where access is controlled by a guard, cipher lock, or card reader), <u>but the use of such measures is not a substitute for physically securing sensitive PII in a locked container when not in use.</u></i></p>
2.4.6	11	<p>Edited the entire section: <i>Do not leave Sensitive PII unattended on a <u>desk</u>, network printer, <u>faesimile fax machine</u>, or copier. Do not send Sensitive PII to a <u>faesimile fax machine</u> without contacting the recipient to arrange for its receipt.</i></p>

Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security

Contents

Introduction.....	5
1.0 What Is Sensitive PII?.....	6
1.1 PII That Is Always Sensitive.....	7
1.2 PII That Is Sensitive In Certain Contexts	8
1.3 Alien Files and Alien Numbers.....	8
2.0 How Must You Safeguard Sensitive PII?	9
2.1 Collect Sensitive PII Only as Authorized	9
2.2 Limit Use of Sensitive PII.....	9
2.3 Minimize Proliferation of Sensitive PII	10
2.4 Secure Sensitive PII	10
3.0 What Must You Do If You Suspect an Incident?	12
3.1 Report a Privacy Incident to Your Supervisor as Soon as It Is Suspected or Confirmed	12
3.2 Do Not Further Compromise the Information	12
Appendix A: Encrypting a File	14
Appendix B: Frequently Asked Questions	16
How can I protect Sensitive PII	16
In the office?	16
On a portable device, such as a laptop and BlackBerry, while traveling?.....	16
In email or other electronic transfer?	17
When sending via facsimile (fax)?	17
In interoffice mail?.....	17
In the mail?	17
When mailing to overseas offices?	18
On my office shared drive?.....	18
How can I minimize my use of Sensitive PII?.....	18
Why shouldn't I store Sensitive PII on unauthorized equipment?	19
How do I secure Sensitive PII that cannot be encrypted, such as paper copies or magnetic tapes?.....	19
What are my responsibilities when requesting or receiving Sensitive PII?.....	19
When should I destroy copies of Sensitive PII materials?.....	20
How should I dispose of Sensitive PII?	20
Notes	21

Introduction

As someone who works for or on behalf of the Department of Homeland Security (DHS), it is your responsibility to protect information that has been entrusted to the Department. An important part of this duty is to ensure that you properly use, protect, and dispose of **personally identifiable information (PII)**.

DHS defines **PII** as *any information that permits the identity of an individual to be directly or indirectly inferred, including any information which 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.*

Some PII is not sensitive, such as the PII on a business card. Other PII is **Sensitive Personally Identifiable Information (Sensitive PII)**, such as a Social Security number or alien number (A-number), and requires stricter handling guidelines because of the increased risk to an individual if compromised.

DHS defines **Sensitive PII** as *personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.*

This Handbook on Safeguarding Sensitive PII at DHS provides minimum standards that apply to every DHS employee, contractor, detailee, and consultant.¹ Your Component Privacy Officer, Program Office, or System Owner may set additional or more specific rules for handling PII, including Sensitive PII, based on the sensitivity of the information involved. Your supervisor or Component Privacy Officer will be able to direct you to your Component-specific rules.

This Handbook explains:

- how to identify Sensitive PII,
- how to protect Sensitive PII in different contexts and formats, and
- what to do if you believe Sensitive PII may have been compromised.

Additionally, Appendix A of this Handbook gives instructions on how to encrypt a file, and Appendix B provides answers to frequently asked questions on specific procedures for protecting Sensitive PII. This is the first version of the Handbook; updates to this document will be issued by the Privacy Office periodically.

A key part of the DHS mission to protect the homeland is to minimize our impact on individual privacy, which is why it is your responsibility to protect Sensitive PII. By upholding your responsibilities, you promote a greater awareness of privacy throughout the Department. If you have any questions or concerns about privacy at DHS, you are encouraged to contact your Component Privacy Officer, Component Privacy Point of Contact (PPOC), or the DHS Privacy Office² at (703) 235-0780 or privacy@dhs.gov. A list of Component Privacy Officers and PPOCs is available at the Chief Privacy Officer's page on the DHS intranet.

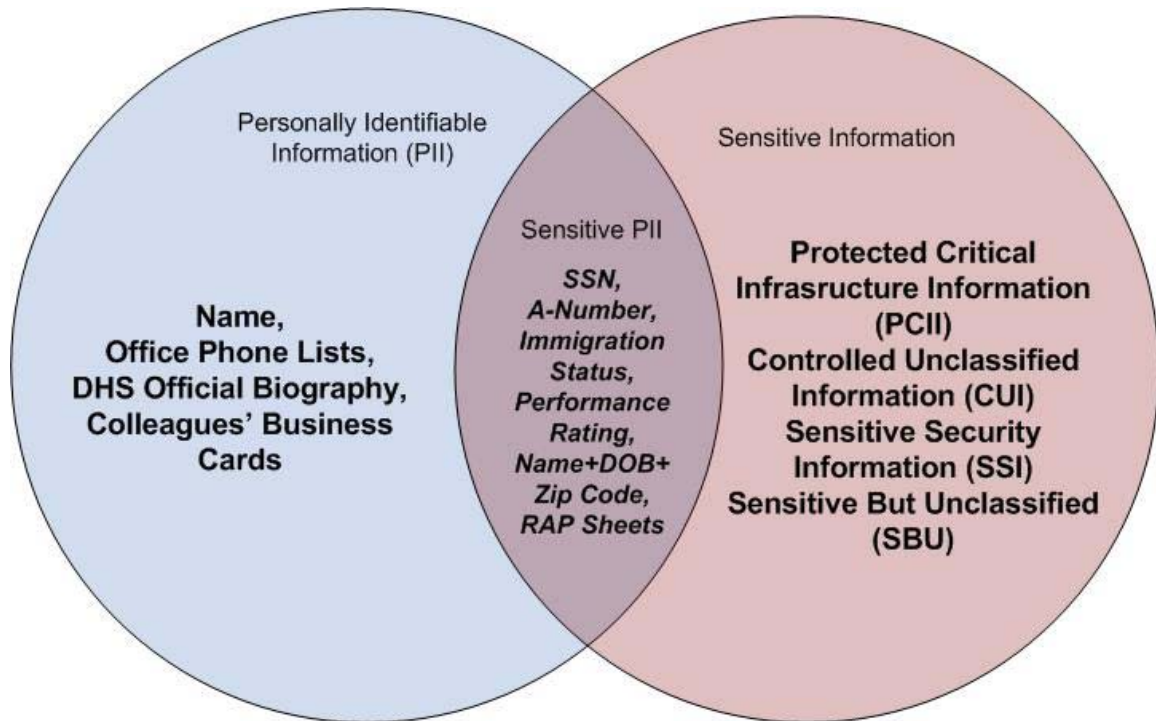
1.0 What Is Sensitive PII?

Sensitive PII is *personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual*. Some categories of PII, when maintained by DHS, are sensitive as stand-alone data elements. Examples of such Sensitive PII include: Social Security number (SSN), alien registration number (A-Number), or biometric identifier. Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of employee names with poor performance ratings.

Not all PII is sensitive. For example, information on a business card or in a public phone directory of agency employees is PII, but in most cases not Sensitive PII, because it is usually widely available public information.

PII that is available to the public or that resides on test and development environments is still considered Sensitive PII in certain circumstances. For example, an individual's SSN might be available in a public record maintained by a local court; however, DHS would still consider that individual's SSN to be Sensitive PII because SSNs are a key identifier used in identity theft and therefore are inherently sensitive. As another example, a DHS employee might maintain a public website identifying herself as having a certain medical condition; however, that same medical information in that employee's personnel file at DHS would still be considered Sensitive PII.

Figure 1.0: Examples of Sensitive Personally Identifiable Information



1.1 PII That Is Always Sensitive

1.1.1 The following personal identifiers, when maintained by DHS, are Sensitive PII even if they are not coupled with additional PII or contextual information:

- complete (9-digit) SSN
 - DHS continues to review and reduce its use of SSNs³ because they are especially sensitive identifiers that can increase individuals' risk of identity theft if compromised. DHS programs and offices should minimize access to, use of, and or display of SSNs wherever possible.⁴
- biometric identifiers (e.g., fingerprint, iris scan, voice print)⁵

1.1.2 The following information is Sensitive PII when grouped with the person's name or other unique identifier, such as address or phone number:

- citizenship or immigration status
- medical information
- driver's license number
- passport number
- full date of birth
- authentication information such as mother's maiden name or passwords
- portions of SSNs such as last four digits⁶
- financial information such as account numbers

- other data created by DHS to identify or authenticate an individual's identity, such as a fingerprint identification number (FIN) or Student and Exchange Visitor Information System (SEVIS) identification number

1.2 PII That Is Sensitive In Certain Contexts

1.2.1 Context matters. PII that might not include the data elements identified in 1.1 might still be sensitive and require special handling if it could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual.⁷

- For example, a collection of names is:
 - Not Sensitive PII if it is a list, file, query result, etc. of
 - attendees at a public meeting
 - stakeholders who subscribe to a DHS listserv
 - employees and contractors at the DHS Privacy Office
 - Sensitive PII if it is a list, file, or query result of
 - law enforcement personnel, such as investigators, agents, and support personnel
 - employees with poor performance ratings
 - undocumented immigrants awaiting deportation proceedings

1.3 Alien Files and Alien Numbers

1.3.1 You may access and use Alien Files (A-Files) and their associated A-numbers often in fulfilling your duties at DHS.

- In almost all contexts, this information is Sensitive PII and must be safeguarded as such.
- You may also use an A-number as a case number for matters pending before the Department of Justice, Executive Office of Immigration Review and Board of Immigration Appeals, or for immigration matters pending before the federal courts. Nothing in this Handbook is intended to interfere with the practice of agency personnel with respect to the uses of the A-number in these contexts.

1.3.2 When non-DHS staff need to send A-numbers to DHS law enforcement personnel, and it is not feasible or consistent with operational needs to do so using encrypted emails, non-DHS staff may send unencrypted A-numbers to DHS law enforcement personnel in order to fulfill their DHS law enforcement and immigration enforcement duties.

- The known location of the alien is the only other PII that may be included in the unencrypted emails sent to DHS law enforcement personnel from non-DHS staff (e.g., DHS contractors who need to send emails originating outside the DHS firewall).

2.0 How Must You Safeguard Sensitive PII?

You should exercise due care when handling all PII and all information you encounter in the course of your work for DHS. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised. The following handling guidelines apply to everyone working for or on behalf of DHS and explain how you must handle Sensitive PII at DHS.

2.1 Collect Sensitive PII Only as Authorized

2.1.1 Be sure that when you collect Sensitive PII, you have the legal authority to do so and if necessary have a Privacy Act system of records notice (SORN) in place that describes the information.

- If you are electronically collecting or maintaining Sensitive PII, be sure your database or information technology system has an approved Privacy Impact Assessment (PIA) and is in compliance with the Federal Information System Management Act (FISMA).

2.1.2 When collecting Sensitive PII from members of the public, do not create unapproved paper or electronic forms or processes to collect Sensitive PII.

- Collecting personal data from members of the public may trigger separate requirements under Paperwork Reduction Act (PRA).⁸

2.2 Limit Use of Sensitive PII

2.2.1 Only access Sensitive PII when you need to know that information,⁹ that is, when your need for the information relates to your official duties.

- If you work for DHS as a contractor, you must have a nondisclosure agreement (NDA) on file with DHS prior to handling Sensitive PII.¹⁰
- Do not access or share Sensitive PII for entertainment or any other purpose unless it is related to your mission need to know.
- Remember that you must secure Sensitive PII in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.

2.2.2 Only use Sensitive PII for official purposes.¹¹

- Use must be compatible with notices, such as Privacy Act System of Records Notice (SORN), Privacy Impact Assessment (PIA), and Privacy Act Statements provided to the individuals from whom the information was collected. If you are unsure about whether a specific use is appropriate, you should confirm with your supervisor or Component Privacy Officer.¹²
- Do not browse files containing Sensitive PII out of curiosity or for personal reasons.

- 2.2.3 Share Sensitive PII only as authorized.
- You are authorized to share Sensitive PII with another DHS employee or contractor if the recipient's need for the information is related to his or her official duties.
 - You are authorized to share Sensitive PII outside of DHS if there is a published routine use in the applicable Privacy Act SORN. All DHS SORNs are posted on the DHS Privacy Office website (www.dhs.gov/privacy).
 - Refer requests for Sensitive PII from members of the public, the media, or other outside entities to your Component FOIA or Disclosure Officer.¹³

2.3 Minimize Proliferation of Sensitive PII

- 2.3.1 Do not create unnecessary or duplicative collections of Sensitive PII, such as duplicate, ancillary, "shadow," or "under the radar" files. Minimizing proliferation of Sensitive PII helps to keep it more secure and reduces the risk of a data breach.
- If you need to create duplicate copies of Sensitive PII to perform a particular task or project, delete or destroy them when they are no longer needed.
 - Unauthorized replication may constitute an unauthorized or illegal Privacy Act system of records. Your Component Privacy Officer or the Privacy Office should be consulted to provide guidance specific to the situation.
- 2.3.2 When you need to print, copy, or extract Sensitive PII from a larger dataset, target your actions to obtain data on only the specific individuals and the specific data elements you need to perform the task at hand.
- 2.3.3 Follow retention and disposal policies.
- The retention of Sensitive PII extracted from a system is not to extend beyond the records retention schedule or as identified in the applicable SORN or Privacy Impact Assessment (PIA) on dhs.gov/privacy.
 - Use appropriate destruction techniques to dispose of Sensitive PII.
 - Shred (do not recycle) papers containing Sensitive PII.
 - Computer drives and other electronic storage devices should be wiped of Sensitive PII before they are re-issued for use.
 - Until you dispose of Sensitive PII, keep it secured in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.

2.4 Secure Sensitive PII

- 2.4.1 When you handle, process, transmit, and/or store Sensitive PII, you should limit the potential for unauthorized disclosure. To do this, protect against "shoulder surfing," eavesdropping, or overhearing by anyone without a need to know the Sensitive PII.
- 2.4.2 Sensitive PII may be saved, stored, or hosted only on Government equipment (including contractor-owned equipment or system that is approved to be used as a

Government system.)¹⁴

- Note that these rules also apply to individuals on an approved Telework program.¹⁵

- 2.4.3 Do not take Sensitive PII home or to any non-DHS approved worksite, in either paper or electronic format, unless appropriately secured. Sensitive PII in electronic form must be encrypted. Paper documents must be under the control of the employee or locked in a secure container when not in use. Personally owned computers may not be used to save, store, or host Sensitive PII.
- 2.4.4 Physically secure sensitive PII (e.g., in a *locked* drawer, cabinet, or desk; in a safe; or in another locked container) when not in use or not otherwise under the control of a person with a need to know. Sensitive PII may be stored in a space where access control measures are employed to prevent unauthorized access by members of the public or other persons without a need to know (e.g., a locked room or floor, or other space where access is controlled by a guard, cipher lock, or card reader), but the use of such measures is not a substitute for physically securing sensitive PII in a locked container when not in use.
- 2.4.5 When you are emailing Sensitive PII outside of DHS, you must send the Sensitive PII within an encrypted attachment with the password provided separately (e.g., by phone or in person). As a last resort, the password can be sent in a separate email, but never in the same email containing the attachment.
- 2.4.6 Do not leave Sensitive PII unattended on a desk, network printer, fax machine, or copier. Do not send Sensitive PII to a fax machine without contacting the recipient to arrange for its receipt.
- 2.4.7 Store Sensitive PII in shared access computer drives (“shared drives”) only if access is restricted to those with a need to know by permissions settings or passwords.
- 2.4.8 Physically secure Sensitive PII when in transit. Do not mail or courier Sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted. Do not return failed hard drives to vendor for warranty if the device was ever used to store Sensitive PII, but sanitize or destroy the media. For example, do not pack laptops or electronic storage devices in checked baggage. Do not leave them in a car overnight or in plain sight in a parking lot.
- 2.4.9 If someone sends you Sensitive PII in an unprotected manner, you still must secure it once you receive it. If you receive a request to accept Sensitive PII in an encrypted format, you must be able to accept the Sensitive PII in that format so that the sender may comply with his or her requirements to encrypt Sensitive PII.

3.0 What Must You Do If You Suspect an Incident?

*DHS defines a **privacy incident** as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users and for an unauthorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both **suspected and confirmed incidents**, whether intentional or inadvertent, involving PII which raise a reasonable risk of harm.¹⁶*

If at any point you suspect or know that Sensitive PII has been handled in a way that violates this Handbook, or otherwise suspect or know of a privacy incident at DHS, regardless of the reason or severity¹⁷ of the incident, you must:

3.1 Report a Privacy Incident to Your Supervisor as Soon as It Is Suspected or Confirmed

- If your supervisor is unavailable or if there is a potential conflict of interest, report the incident to your Program Manager or Helpdesk.
 - Those officials must report the incident to the Component Chief Information Security Officer (CISO), Information Systems Security Manager (ISSM), and/or Privacy Officer, who then, if necessary, reports the incident to the DHS Security Operations Center (SOC) and proceeds according to the DHS Privacy Incident Handling Guidance (PIHG).¹⁸
- Document or maintain records of information and actions relevant to the incident, as it may be required in the privacy incident handling report.
- Any alleged violations that may constitute criminal misconduct, identity theft or other serious misconduct, or reflect systematic violations within the Department will be reported to the DHS Office of the Inspector General (OIG) as part of the privacy incident reporting process.

3.2 Do Not Further Compromise the Information

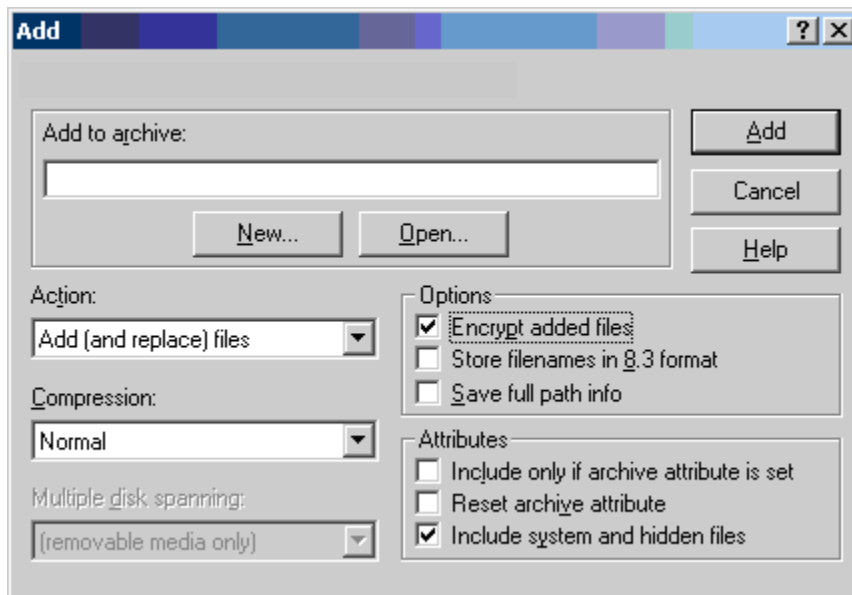
- Beware of these common mistakes so that your response to a privacy incident does not constitute another incident:
 - Do not forward compromised information (e.g., SSN, full name, birth date, etc.) when reporting an incident.
 - If and when the compromised Sensitive PII is needed by your supervisor, PPOC, ISSM, or the Helpdesk in order to respond to an incident, you will be given instructions on whether the compromised information needs to be forwarded to someone at DHS.
 - If you see Sensitive PII in an email that you suspect constitutes a privacy incident, remember that the information is duplicated and further compromised if you forward it, reply, or “reply to all.”
 - Before you reply or forward an email, make sure that you remove any Sensitive PII that should not be disclosed from the email chain below.

- Be careful when “hiding” columns in spreadsheets that contain Sensitive PII. When emailed to a recipient who is not aware that a spreadsheet contains hidden columns, that person may inadvertently forward that spreadsheet to someone who does not need to know that information.

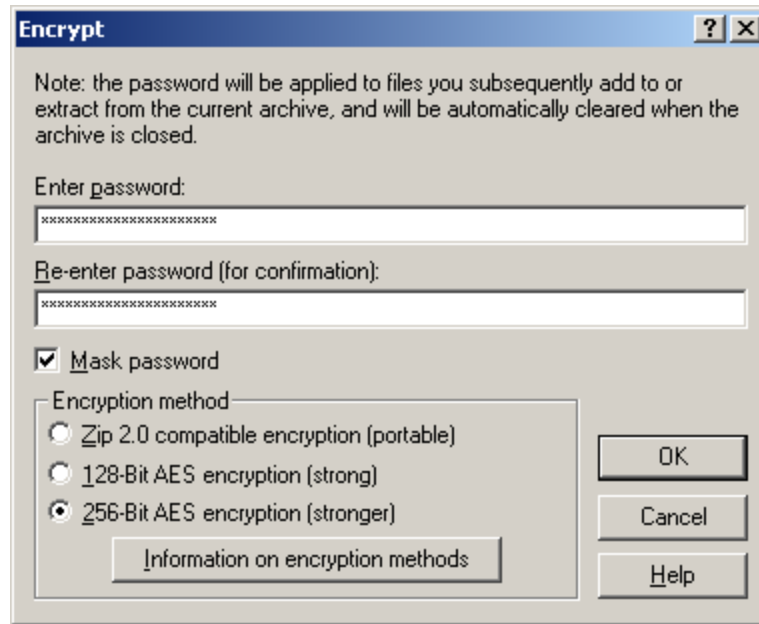
Appendix A: Encrypting a File

To Encrypt a File using WinZip 10.0:

1. Save the file to your hard drive
2. Open up Windows Explorer and locate the file
3. Right click on the file
4. Select “WinZip”
5. Select “Add to WinZip”
6. In the Add box that pops up, in the middle right you will see an “options” area
7. Click the “Encrypt added files” check box



8. Click the “Add” button
9. Check the “Mask Password” checkbox if not already checked
 - a. Enter a string of characters as a password composed of letters, numbers, and special characters (minimum 8 characters – maximum 64)
 - b. Select the 256-Bit AES encryption radio button
 - c. Click “OK”



10. You have successfully encrypted the new Zip file that can now be attached to an email

Sending an encrypted Zip File via email:


1. Compose a new message
2. Attach the Zip File
3. Send message

****In a SEPARATE medium (i.e. by phone or in person), send the password to the recipients of the email. As a last resort, the password can either be sent out by email prior to sending the file, or afterwards, but NEVER in the same email to which the file is attached.****

Appendix B: Frequently Asked Questions

How can I protect Sensitive PII . . .

In the office?

- Position your computer screen so that it is minimally visible to people passing by. Use a privacy screen if you regularly access Sensitive PII in an unsecured area where those without a need to know or members of the public can see your screen, such as a reception area.
- When within earshot of anyone who does not need to know Sensitive PII, avoid discussing that information in person or over the telephone.
- If you must discuss Sensitive PII using a speakerphone, phone bridge or video teleconference, do so only if you are in a location where those without a need to know cannot overhear.
- Keep in mind that phone conversations are easily overheard between cubicles, so Sensitive PII is most securely discussed in an office or conference room behind a closed door.
- Lock your computer when away from your duty station. Depending on your equipment, you may lock your computer by (1) holding down “+ “L”, (2) holding down “Ctrl”+ “Alt” + “Delete” and then hitting “Enter”, or (3) by removing your Common Access Card (CAC) from your machine.
- Do not choose options that allow your computer to remember passwords.
- Remember that some places that seem private still pose a risk for unauthorized disclosure, such as in a taxicab or the DHS shuttle.

On a portable device, such as a laptop and BlackBerry, while traveling?

- Encrypt the entire laptop, or those files containing Sensitive PII, so that Sensitive PII will not be compromised if the laptop is lost or stolen. Encryption can also protect Sensitive PII on flash drives, CDs, or other storage media while traveling.
- Keep the DHS or Component Security Operation Center (SOC) phone number available (not on the portable device) in case of theft, to report the loss immediately. In some cases, the SOC will be able to remotely destroy the data on the device so that it cannot be accessed by an unauthorized user.
- Do not allow Sensitive PII to be visible on your screen (including personal digital assistants such as Blackberries), on paper, or overheard by people in a public place, such as an airport or on the subway.
- At airport security, place your laptop or personal electronic device (PED) such as BlackBerry) on the conveyor belt only after the belongings of the person ahead of you

have cleared the scanner. If you are delayed, keep your eye on the laptop or PED until you can pick it up.

- Do not place the laptop or PED in checked luggage.
- Do not store the laptop or PED in an airport, a train or bus station, or any public locker.
- If you must leave a laptop or PED in a car, lock it in the trunk so that it is out of sight.
- Avoid leaving the laptop or PED in a hotel room. If you must leave it in a hotel room, lock it inside an in-room safe or another piece of luggage.

In email or other electronic transfer?

- Electronic transfers of Sensitive PII outside of the DHS network (e.g., emailing from a DHS email address to a non-DHS email address) must be encrypted.
 - Non-Government equipment that is approved to be operated as if it is a Government system is considered to be inside DHS for this purpose.
 - Sensitive PII does not need to be encrypted if the information has been deemed releasable and is being sent to an individual in response to a Congressional, Privacy Act or Freedom of Information Act (FOIA) request.
 - See Appendix A for instructions on how to encrypt a file using WinZip version 10. Using WinZip is one way to encrypt Sensitive PII. Your Component may have other recommended tools and methods for encrypting information.
- Unless your Component or office has published a requirement to the contrary, you may electronically transfer Sensitive PII within the DHS network without encrypting it. However, when one email or electronic transfer contains a large volume of Sensitive PII, it is advisable to send the Sensitive PII within a password protected attachment with the password provided under separate cover, such as in person, by phone, or in a separate email. This extra measure can mitigate the risk of a large volume of Sensitive PII being accidentally forwarded outside DHS in an unencrypted format.

When sending via facsimile (fax)?

- When faxing Sensitive PII, the sender should alert the recipient prior to faxing so that the recipient can ensure that the transmission is not left unattended.

In interoffice mail?

- Sensitive PII should be sent as accountable mail (blue messenger envelopes)¹⁹ furnished by your onsite DHS mailroom or by DHS courier. The sender should verify that the recipient received the information.

In the mail?

- For mailings containing a small amount of Sensitive PII materials (such as individual employee actions):

- Seal Sensitive PII materials in an opaque envelope or container.
- Mail Sensitive PII materials using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service (e.g., DHL).
- For large data extracts, database transfers, backup tape transfers, or similar collections of Sensitive PII:
 - Encrypt (if possible) and use a receipted delivery service (i.e. Return Receipt, Certified or Registered mail) or a tracking service (e.g., "Track & Return.") to ensure secure delivery is made to the appropriate recipient.

When mailing to overseas offices?

- When serviced by a military postal facility (i.e., Army Post Office/Fleet Post Office), send Sensitive PII materials directly to the office via the U.S. Postal Service's First Class Mail.
- Where the overseas office is not serviced by a military postal facility, send the Sensitive PII materials through the Department of State diplomatic courier.

On my office shared drive?

- Store in a way that limits access to only those with a need to know. For example, if Sensitive PII needs to be stored on a shared network folder, create a limited-access sub-folder to store that data and provide access privileges to only those who have an official need to access the data.

How can I minimize my use of Sensitive PII?

- Whenever possible, minimize the duplication and dissemination of files and papers containing Sensitive PII.
- If you need to use a unique number or data element to identify individuals, use email addresses or case record numbers instead of Social Security numbers.
- Only print, extract, and copy Sensitive PII when the risk is justified by an official need that is not easily met using other means.
 - For example, if you need to generate a list of employees in a particular office and their salaries for a project, query the payroll database to return to you only those employees' names and salaries (and not, for example, other sensitive data such as SSNs). If you cannot customize the reports generated by a database, often you can load the results into an Excel spreadsheet and delete the data you do not need before saving it and distributing it to others.
 - When using paper copies, you can redact Sensitive PII that is not necessary for your immediate use or for a recipient to see.
 - Some legacy IT systems have "canned" reports that may not allow you to exclude data elements. One way to address this would be to delete those elements you do not need once the extract is provided. For example, many automated report outputs are formatted as spreadsheets, where columns of types of data elements may be easily deleted.

Why shouldn't I store Sensitive PII on unauthorized equipment?

- DHS issued or approved portable media devices, such as laptops, USB drives, and external hard drives, are encrypted.²⁰ Encryption protects the data on the device from being accessed by an unauthorized user if the device is lost or stolen.
- Non-Government equipment may have unauthorized software or allow access to an unauthorized person, which risk bringing computer viruses, spyware, or other technology that may cause harm to the DHS network and could allow unauthorized access to DHS information, including Sensitive PII.

How do I secure Sensitive PII that cannot be encrypted, such as paper copies or magnetic tapes?

- Sensitive PII stored on portable electronic media that cannot be encrypted (such as magnetic tapes) or in hard copy must be stored in a locked compartment, such as filing cabinet or desk drawer.

What are my responsibilities when requesting or receiving Sensitive PII?

- When collecting Sensitive PII from members of the public, use only an OMB-approved²¹ paper or electronic form and collect Sensitive PII directly from the individual to the extent possible.
 - For example, if a DHS employee needs to submit information about a visitor to have him or her cleared to enter a DHS facility, the *visitor* should fill out his or her portion of the approved visitor form directly wherever possible.²² This will limit unnecessary proliferation of that individual's personal data, but will also allow him or her to be aware of what information is being collected, to consent to releasing that information, and to receive notice required by the Privacy Act of the uses and purpose for collection of the information.
- If you receive Sensitive PII electronically on behalf of DHS, you must at the sender's request be able to accept the Sensitive PII in encrypted format so that the sender may comply with their own requirements to encrypt sensitive data.
 - You may require senders to use an encryption program (such as WinZip) that allows you to decrypt without acquiring additional software.
 - If someone sends you Sensitive PII in an unprotected manner, you still must protect that data in the same manner as all Sensitive PII you handle once you receive it.
 - For example, if someone outside of DHS sends you his or her unsecured Sensitive PII in the body of an email, you must encrypt that data if you wish to email it to another non-DHS recipient.
 - As a best practice, every request you make for Sensitive PII should be accompanied by a reminder of how to properly secure the information. DHS suggests the following reminder when requesting information from someone outside of DHS:

“The information I have requested is Sensitive Personally Identifiable Information. To properly secure this information, please send it within an encrypted attachment with the password provided under a separate cover, such as in person, by phone, or in a separate email.”

When should I destroy copies of Sensitive PII materials?

- Sensitive PII, including archived emails²³ containing Sensitive PII, shall be destroyed when retention of the data is no longer required, consistent with applicable record retention schedules²⁴ or as identified in the applicable system of records notice (SORN) published in the *Federal Register* or Privacy Impact Assessment (PIA) on dhs.gov/privacy.

How should I dispose of Sensitive PII?

- Printed material can be destroyed using an approved shredder, “burn bags,” or equivalent destruction means. Do not use recycle bins for this purpose.
- Remember to also secure Sensitive PII that has been discarded in burn bags that are awaiting removal, shredding, or destruction.
- All Sensitive PII on diskettes must be permanently erased or destroyed according to your ISSM’s standards before re-use.
- Mobile devices containing Sensitive PII must be sanitized according to your ISSM’s standards when no longer needed by an employee.

Notes

¹ As required by OMB M-07-16, these rules also apply to DHS licensees, certificate holders, and grantees who handle or collect PII, including Sensitive PII, for or on behalf of DHS.

² Pursuant to Section 222(a) of the Homeland Security Act of 2002, as amended, the DHS Chief Privacy Officer assumes primary responsibility for implementing privacy policy at DHS.

³ DHS and other Federal agencies are working to minimize the use of Sensitive PII, but many processes related to personnel practices and procedures will still require the use of items such as date of birth and SSN in the interim. Further, Executive Order 9397 mandates the SSN as the Federal employee ID number. This means that any type of recordkeeping that requires an employee ID number currently requires SSN, including several human resources and training IT systems.

⁴ For more information on using Social Security numbers at DHS, see Privacy Policy Guidance Memorandum 2007-02 *Regarding Use of Social Security Numbers at the Department of Homeland Security*, June 4, 2007 under the Privacy Policy Guidance and Reports link at www.dhs.gov/privacy.

⁵ The Intelligence Reform and Terrorism Prevention Act of 2004 defines *biometric identifier information* as “the distinct physical or behavioral characteristics of an individual that are used for unique identification, or verification of the identity, of an individual.” Examples of biometrics include a person’s fingerprint, voiceprint, or iris scan.

⁶ Because of the numbering scheme used to assign SSNs, the first five digits of the nine-digit number can in many cases be extrapolated from a person’s place and date of birth. This means that in some cases, the last four digits of the SSN plus additional information may permit the entire SSN to be known. For more information, see *The SSN Numbering Scheme* at <http://www.ssa.gov/history/ssn/geocard.html>.

⁷ Subsection (e)(10) of the Privacy Act of 1974, as amended (5 USC § 552a) states that “[e]ach agency that maintains a system of records shall...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”

⁸ For more information about the Paperwork Reduction Act (PRA) (44 U.S.C. 3501 et seq.), contact the DHS PRA Program Office at DHSPRA@hq.dhs.gov.

⁹ DHS Management Directive 11042.1: *Safeguarding Sensitive But Unclassified (For Official Use Only) Information* defines need to know as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized Governmental function, i.e., access is required for the performance of official duties.

¹⁰ NDAs are generally obtained from DHS contractors prior to those individuals being issued a badge and/or access to DHS systems, as part of the security on boarding process.

¹¹ Where a system of records notice (SORN) has been published for a DHS system, the SORN identifies the official purposes for which the PII, including Sensitive PII, was collected.

¹² Depending on your role in the Department, the appropriate supervisor may be your Program Manager, Director, Privacy Officer, or ISSM. You are also encouraged to contact the DHS Privacy Office at privacy@dhs.gov if you need assistance locating the person who can respond to your privacy questions, have privacy issues that need escalation, clarification, or resolution, or if you need your concern to be kept confidential. Also, you should refer to the DHS Office of Inspector General (OIG) any alleged violations of the terms of this document that may constitute criminal misconduct, identity theft, or other serious misconduct, or reflect systemic violations within the department. You can contact the OIG by writing to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528. You can also fax the information to (202) 254-4292, or email DHISOIGHotline@dhs.gov.

¹³ If you are unsure to whom to refer the request, contact your supervisor or the FOIA office at FOIA@dhs.gov.

¹⁴ DHS Sensitive Systems Policy Directive 4300A, section 4.8.3 (b) states that “equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component ISSM.”

¹⁵ DHS Management Directive 3070.2, *Telework Directive*, specifies that “[t]eleworking employees are subject to ensuring that records subject to Privacy Act and sensitive or classified data are not disclosed to anyone except those who are authorized access to such information in order to perform their duties.”

¹⁶ A reasonable risk of harm means a likelihood that an individual may experience a substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. For example, the loss of someone’s business card does not pose a reasonable risk of harm. You should consult your PPOC or the Privacy Office for assistance in determining a privacy incident.

¹⁷ It is useful to note that reported privacy incidents are evaluated based on low, moderate, or high impact or risk. DHS responds to the incident according to its potential severity. If there is a reasonable risk of harm, the incident must be reported even if that harm would have a low impact.

¹⁸ For more information on what DHS does when there is a privacy incident, see the DHS Privacy Incident Handling Guidance (PIHG) available at dhs.gov/privacy.

¹⁹ For more information on accountable interoffice mail, see the *Outgoing Mail Policies and Services* section of the DHS Executive Secretariat Handbook or contact the DHS mailroom. If your office does not participate in DHS HQ interoffice mail, consult your supervisor for your local accountable interoffice mail procedures.

²⁰ OMB Memorandum M-06-16 requires that all agencies “[e]ncrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing.” Encryption of all mobile computing devices is required by *DHS Sensitive Systems Policy Directive 4300A*. If you are issued a portable media device which you believe may not be encrypted, contact your component ISSM.

²¹ See OMB Office Of Information And Regulatory Affairs *Inventory Of Approved Information Collections* at www.whitehouse.gov/omb for a list of OMB-approved forms.

²² Subsection (e)(2) of the Privacy Act of 1974, as amended (5 USC § 552a) states that “[e]ach agency that maintains a system of records shall...collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs.”

²³ Archived emails in this context include only those that the user manages, not those saved as part of system backups by system administrators.

²⁴ For questions about record retention schedules, contact your Component Records Officer or DHSRecordsManagement@HQ.DHS.GOV.

*The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Phone: 703-235-0780
Email: privacy@dhs.gov*

www.dhs.gov/privacy