



Handbook for Safeguarding Sensitive PII

Privacy Policy Directive 047-01-007, Revision 3

Published by the DHS Privacy Office

December 4, 2017



Homeland
Security

Table of Contents

Introduction	3
Authorities	7
Definitions	7
PII and Sensitive PII Defined	5
Additional Definitions	7
Collecting Sensitive PII	8
Proper Authorization is Needed	8
Best Practices	8
Collection of PII via Mobile Applications	10
Storing Sensitive PII	11
IT Systems	11
Internal Websites and Shared Network Drives	11
Using Sensitive PII	12
Proper Authorization is Needed	12
Best Practices	12
<i>Equipment</i>	12
<i>Paper</i>	13
<i>In Transit</i>	13
<i>Teleworking</i>	13
Disseminating Sensitive PII — Information Sharing	14
Proper Authorization is Needed	14
Unauthorized Dissemination of Sensitive PII	15
<i>Social Engineering</i>	15
<i>Phishing</i>	15
Best Practices	15
<i>Email</i>	16
<i>Mail</i>	17
<i>Equipment</i>	17
Disposing of Sensitive PII	18
Reporting a Privacy Incident	19
Resources	20

Introduction

In its mission to secure the Homeland, the Department of Homeland Security (DHS) collects personal information, also known as **Personally Identifiable Information (PII)**, from U.S. citizens, Lawful Permanent Residents (LPR), visitors to the U.S., and employees or contractors to the Department. As an employee, contractor, appointee, detailee, intern, or consultant (hereafter referred to as "DHS staff"), you are obligated by law and by DHS policy to protect PII to prevent identity theft or other adverse consequences, such as a privacy incident, compromise, or misuse of data.

You should exercise care when handling all PII. **Sensitive PII (SPII)**, however, requires special handling due to the increased risk of harm to an individual if it is compromised. The loss or compromise of SPII can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and in rare cases, a risk to personal safety.

This Handbook provides best practices and DHS policy requirements to prevent a privacy incident involving PII/SPII during all stages of the information lifecycle: *when collecting, storing, using, disseminating, or disposing of PII/SPII.*

This handbook explains:

- how to identify PII and SPII,
- how to protect PII and SPII in different contexts and formats, and
- what to do if you believe PII and/or SPII has been lost or compromised.

Most privacy incidents at DHS are accidental, so by following these guidelines, you can help to prevent them.

Please note that your Component Privacy Officer, Privacy Point of Contact (PPOC), Program Office, or System Owner may establish additional or more specific rules for handling PII/SPII based on the sensitivity of the information involved.



Questions

A complete list of DHS Component Privacy Office contacts can be found on our website: www.dhs.gov/privacy.

Authorities

All DHS staff are obligated to safeguard PII/SPII, as described in numerous federal statutes, regulations, agency-wide directives, and DHS policies, of which the following is a sampling:

Federal Statutes

- [5 U.S.C. § 552a, Privacy Act of 1974, as amended](#)
- [5 U.S.C. § 552a \(note\), Judicial Redress Act of 2015](#)
- [5 U.S.C. § 552, Freedom of Information Act \(FOIA\)](#)
- [6 U.S.C. § 142, Homeland Security Act, Privacy Officer](#)
- 44 U.S.C. 3501 et seq., [Paperwork Reduction Act](#) (PRA)
- E-government Act of 2002 (Public Law 107-347)

OMB/Government-wide Guidance

- Office of Management and Budget (OMB) [Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information](#) (January 2017)
- [OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act](#) (December 2016)
- [OMB Circular No. A-130, Managing Information as a Strategic Resource](#) (July 2016)

DHS Policy

- [DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified \(For Official Use Only\) Information](#);
- [DHS Management Instruction 123-05-001, Telework Program](#)
- [DHS Privacy Policy Instruction 047-01-008, DHS Privacy Incident Handling Guidance](#), (November 2017)
- [DHS Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information](#) (April 2017)
- [DHS Policy Directive 121-07, Standard Procedures When Restricted Personal Information is Posted On the Internet or Social Media \(Doxxing\)](#) (April 2016)
- [DHS Privacy Policy Instruction 047-01-003 for DHS Mobile Applications](#) (March 2016)
- [DHS Privacy Policy Instruction 047-01-006, Privacy Incident Responsibilities and Breach Response Team](#) (December 2017)
- [DHS Sensitive Systems Policy Directive 4300A](#) and [DHS 4300A Sensitive Systems Handbook](#);
- [DHS Privacy Policy Directive 110-01](#) and [Instruction 110-01-001, Operational Use of Social Media](#)
- [DHS Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security](#) (December 2008);
- [DHS Privacy Policy Directive 140-11, Use of Social Security Numbers at the Department of Homeland Security](#) (June 2007).

Definitions

PII and Sensitive PII Defined

DHS defines personal information as “**Personally Identifiable Information**” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

PII is a form of **Sensitive Information**,¹ which includes, but is not limited to, PII and Sensitive PII.

Sensitive PII (SPII) is *Personally Identifiable Information*, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

SPII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised. Some categories of PII are sensitive as stand-alone data elements, including your Social Security number (SSN) and driver's license or state identification number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.

See the table on the next page for more examples of PII and SPII.

- When determining the sensitivity of PII, agencies should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of data fields together.
 - ⇒ For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or zip code.
- PII can become more sensitive when combined with other information.
 - ⇒ For example, name and credit card number are more sensitive when combined than apart.
 - ⇒ Generally non-SPII, such as a name, might become sensitive in certain contexts, such as on a clinic's patient list.



1. *Sensitive Information* is any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. See DHS Sensitive Systems Policy Directive 4300A, version 13.1, July 27, 2017.

Context matters. This table should not be regarded as an all-inclusive list of sensitive data elements. Context is also important in determining the sensitivity of PII. PII that might not include the data elements identified may still be sensitive and require special handling if its compromise could cause substantial harm, inconvenience, embarrassment, or unfairness to an individual.

For example, a collection of names:

- Is **not** SPII if it is a list, file, query result of:
 - ⇒ attendees at a public meeting or
 - ⇒ stakeholders who subscribe to a DHS email distribution list

- **Is** SPII if it is a list, file, query result of:
 - ⇒ law enforcement personnel, such as investigators, agents, or support personnel, or
 - ⇒ employee performance ratings, or
 - ⇒ employees with overdue mandatory training course completions

What is PII?
PII includes your name and your work email, address, and phone
What is Sensitive PII?
STAND ALONE
• Social Security numbers
• Driver's license or state ID numbers
• Passport numbers
• Alien Registration numbers
• Financial account numbers
• Biometric identifiers
IN COMBINATION
• Citizenship or immigration status
• Medical information
• Ethnic or religious affiliation
• Personal email, address, and
• Account passwords
• Last 4 digits of the SSN
• Date of birth
• Criminal History
• Mother's maiden name

9. See footnote 1, *supra*, for the definition of "privacy incident."

Additional Definitions

Fair Information Practice Principles (FIPP)²

The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of PII. DHS uses the FIPPs to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill DHS's mission, and how to best apply privacy protections in light of these principles. These eight principles are:

1. **Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII.
2. **Individual Participation:** DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
3. **Purpose Specification:** DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
4. **Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitation:** DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
6. **Data Quality and Integrity:** DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
7. **Security:** DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Information life cycle:³ The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

2. See DHS Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 29, 2008). See also DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 27, 2017).

Need to Know: Refers to an exception under the Privacy Act that authorizes disclosures of Privacy Act protected records within an agency to agency staff to fulfill their job responsibilities for necessary, official agency purposes and mission needs. See 5 U.S.C. § 552a(b)(1). For disclosures not covered by the Privacy Act, access to the information must be necessary for a person to conduct his or her official duties. This is separate from whether the person has all the necessary official approvals (such as a security clearance) to access certain information. *We recommend you consult your supervisor or Component Privacy Officer or PPOC to determine if an individual seeking access to PII/SPII has a need to know.*

Privacy Incident:⁴ The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII; or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, in either paper or electronic format, whether intentional or inadvertent, which raise a reasonable risk of harm.



-
3. As defined in OMB Circular No. A-130. See *Authorities*.
 4. DHS changed its long standing definition of privacy incident to comport with OMB's definition of a **breach** in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of PII* (Jan. 3, 2017), but added the final sentence to address suspected and accidental incidents. We kept the term "privacy incident" to be consistent with other DHS incident types.

Collecting Sensitive PII

Proper Authorization is Needed

Consistent with the FIPPs, be certain of the following before collecting or maintaining PII/SPII:

1. You have the legal authority to collect the specific information;
2. The data collection is covered by a Privacy Act System of Records Notice (SORN), if necessary; and
3. The database or information technology (IT) system is covered by an approved Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA), if necessary.
4. **Social Media:** The Department engages in the operational use of social media⁵ only as authorized by DHS privacy policy, privacy laws applicable to DHS, applicable Federal Government-wide policies, and other applicable statutory authorities. Consult [DHS Privacy Policy Instruction 110-01-001 for the Operational Use of Social Media](#), and your Component Office of Public Affairs, Privacy Officer or PPOC for additional guidance.

For more information on DHS privacy compliance documentation, please consult our [website](#).

Best Practices

When collecting PII/SPII from members of the public, ensure that all paper or electronic forms or processes are reviewed and approved by the DHS Forms Management Office (forms@hq.dhs.gov) prior to collection, and if possible, only collect PII/SPII directly from the individual.⁶ Collecting personal information from members of the public may trigger separate requirements under the Paperwork Reduction Act (PRA),⁷ and may also require that the form contain a Privacy Act Statement (see 5 U.S.C. § 552a(e)(3)) by law or a separate Privacy Notice⁸ by policy to provide transparency and notice to the person about whom PII/SPII is being collected, and describe how the Department will use their PII/SPII. Additionally, a Forms Privacy Threshold Analysis should be completed on all forms, whether they be DHS-owned or from another agency, like OPM. Please contact your Component Privacy Office for instructions.

- Consistent with the FIPP on data minimization, you should only collect PII that is directly relevant

-
5. "Operational use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings.
 6. For example, subsection (e)(2) of the Privacy Act of 1974, 5 U.S.C. § 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."
 7. For more information about the Paperwork Reduction Act (PRA), 44 U.S.C. 3501 et seq., contact the DHS PRA Program Office at DHS.PRA@hq.dhs.gov.
 8. Privacy Act Statements should only be used when the information collection is from U.S. citizens or Lawful Permanent Residents (LPR). Because Privacy Act rights are no longer granted to non-U.S. Citizens/non-LPRs, a form that collects information regarding such individuals should have a Privacy Notice pursuant to DHS policy.

and necessary to accomplish the specified purpose, retain PII only for as long as necessary to fulfill the specified purpose, and destroy it when permitted to do so, in accordance with the applicable records retention schedule.

⇒ **Social Security numbers:** DHS programs shall only collect, use, maintain, and disseminate SSNs when required by statute or regulation, or pursuant to a specific authorized purpose. Absent these requirements, DHS programs shall not collect or use an SSN as a unique identifier; rather, programs should create their own unique identifiers, or use a different piece of information to identify or link information concerning an individual. If you need to use a unique number or data element to identify individuals, the DHS Privacy Office suggests using email addresses or case record numbers instead of SSNs.

- Provide instructions to the individual, as appropriate, on how to properly submit SPII, for example:
 - ⇒ *“The information requested is Sensitive Personally Identifiable Information. To properly secure this information, please email it to me within an encrypted or password-protected attachment, and email the password separately.”*

Collection of PII via Mobile Applications

As the use of mobile technology to send and receive information becomes more prevalent, DHS has begun to develop and deploy mobile applications, also known as “mobile apps,” for use by the public and by DHS staff.

Mobile apps present privacy risks that are unique to mobile app technology. The risks involve how PII, SPII, and other sensitive content such as location information, third party data, mobile device identifiers, and metadata are collected, stored, used, and shared. Additionally, mobile devices and mobile apps may be more vulnerable to Internet security threats, which could potentially compromise a user’s information, and even pose a threat to DHS systems.

To address these concerns, the DHS Privacy Office issued [Instruction 047-01-003, Privacy Policy for DHS Mobile Applications](#) to ensure that appropriate privacy protections are incorporated into mobile apps developed by, on behalf of, or in coordination with the Department. The policy also requires that DHS mobile apps be run through the DHS “Carwash” process, which scans the application’s code to ensure that it does not contain privacy or security vulnerabilities.



Storing Sensitive PII

IT Systems

Once collected, SPII should be stored based on the specifications for either electronic or paper storage outlined in the SORN, if necessary and applicable, under the section titled: *Policies and Practices for Storage of Records*. Databases or IT systems storing SPII should employ technical safeguards and access controls to restrict access to staff with an official need to know the Sensitive Information. The same rule applies to PII (not just SPII) stored in the cloud. Be sure to consult the Program Manager for specific guidance on storage and access controls for the applicable system or program.



Internal Websites and Shared Network Drives

When saving or posting SPII on shared network drives, SharePoint collaboration sites, or Outlook calendars, follow these guidelines:

Shared Network Drives

Shared network drives must have access restrictions in place so only individuals with an official need to know can access SPII saved on them. Contact your Help Desk for instructions.

SharePoint Collaboration Sites

All collaboration sites must display visual cues indicating whether SPII is authorized to be posted. DHS Components may build more detailed controls and technical enhancements into their respective collaboration sites, so please contact your Component Privacy Officer or PPOC before establishing a new collaboration site that will contain SPII. A PTA may also be required.

Outlook Calendars

It is best to avoid posting SPII on your Outlook Calendar, but if you absolutely need to, always activate Microsoft Outlook's "Private" feature to mark a meeting or appointment containing SPII as "Private" so that other people who do not have an official need to know, but have access to your calendar, cannot see details of the item. For example, do not post information regarding confidential personnel matters. Also, do not include SPII in the subject line of a meeting or appointment.

Using Sensitive PII

Proper Authorization is Needed

Access or use of SPII is only permitted when you have an official *need to know* the information, that is, when the information relates to your official duties. As stated above, databases or IT systems storing SPII should employ technical safeguards and access controls to restrict access to staff with an official need to know the Sensitive Information. Never browse files containing SPII out of curiosity or for personal reasons.

Guidance and Training

Use of PII must be compatible with the purpose stated in DHS notices, such as a SORN, PIA, Privacy Act Statement, or, for those not covered by the Privacy Act, a Privacy Notice 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 Component Privacy Officer or PPOC.

In addition, prior to accessing SPII, all DHS staff, including contractors, must complete onboarding privacy awareness training and the mandatory online privacy awareness course, *Privacy at DHS: Protecting Personal Information*, available on all Component Learning Management Systems.⁹ Online privacy training must be completed annually.

Finally, contractors are required to follow Federal Acquisition Regulation (FAR) provisions when handling PII and SPII (see, e.g., Title 48 of the Code of Federal Regulations (CFR), Federal Acquisition Regulations System). Moreover, the Department has established policies and procedures for how contractors should handle SPII (e.g., [Management Directive 11042.1, Safeguarding Sensitive But Unclassified \(For Official Use Only\) Information.](#))

Best Practices

When accessing or using SPII, take proactive steps to prevent a privacy incident.¹⁰

Equipment

SPII may only be accessed, viewed, saved, stored, or hosted on DHS-approved, encrypted portable electronic devices (PEDs), such as laptops, tablets, and smartphones, as well as encrypted government-issued USB flash drives, CDs, DVDs, and external hard drives. Personally-owned equipment and software cannot be used to process, access, or store sensitive information without the written prior approval of the DHS CISO.¹¹

All portable media must be encrypted pursuant to *DHS Sensitive Systems Policy Directive 4300A*, and kept locked and secured while unattended at work, teleworking, and in transit.

- Protect against “shoulder surfing” when viewing SPII on your PED.
- Never share user names, passwords, or PIV cards with anyone, including co-workers.

9. Onboarding privacy training is mandated by OMB Circulars A-130 and A-108, and annual online privacy training is mandated by OMB Memorandum M-17-12.

10. See definition of a privacy incident on page 7.

11. Pursuant to DHS Sensitive Systems Policy Directive 4300-A, version 13.1, July 27, 2017.

Paper

Physically secure SPII (e.g., in a *locked* office, drawer, cabinet, desk, or safe) when not in use.

- *Never* leave SPII unattended on a desk, network printer, fax machine, or copier.
- Avoid sending SPII using a fax machine unless you can confirm the fax is sent directly to the intended recipient. If possible, scan, encrypt, or password-protect the document, and email it instead.
- Protect against "shoulder surfing" or eavesdropping by being aware of your surroundings when processing or discussing SPII and employee or contractor personnel data.
- Consider using a Privacy Data coversheet when handling hard copy SPII.

In transit

Obtain authorization from your supervisor before removing electronic or hard copy documents containing SPII from the workplace.

- Do not take SPII home or to any non-DHS approved worksite in either paper or electronic format, unless appropriately secured.
- Never perform official work on your laptop or tablet while on mass transit (e.g., train, plane) where SPII may be viewed by shoulder surfers who do not have a need to know. Furthermore, working while in transit increases the risk for equipment and documents to be left behind and then compromised.
- Do not leave your PED in a car. If lost or stolen, immediately report it as a lost asset according to your Component's reporting procedures, and inform your supervisor.
- When traveling by plane, never place your PED inside of your checked luggage, unless TSA officials instruct you otherwise.

Teleworking

Consult the three previous sections under Best Practices above, as well as [DHS Management Instruction 123-05-001, Telework Program](#).

- Do not transfer files to your home computer or print agency records on your home printer.
- Never use your personal email to conduct official business. Contractors should not utilize contractor email addresses to conduct DHS business unless specifically authorized by the contract.
- Do not send emails containing SPII to or from your personal email account, or to another person's personal email account.
- Obtain authorization from your supervisor to remove electronic or hard copy documents containing SPII from the workplace.
- Secure your PED and any hard copy SPII while teleworking, and ensure that any other household members cannot access them. For example, in a locked home office, file cabinet, drawer, or hotel safe.

Disseminating Sensitive PII — Information Sharing

Proper Authorization Is Needed

Internally

You are authorized to share SPII with other DHS staff only if the recipient has an official need to know, and/or the person whose SPII is being shared consents to the sharing.

Externally

You are authorized to share PII outside of DHS if:

1. The person whose PII is being shared requests or consents to the sharing; or
2. The recipient's need for the information is related to his or her official duties; and
3. If the PII is contained in records covered by a system of records, there must be an authorized disclosure exception (e.g., a published routine use in the applicable SORN¹²) that permits sharing pursuant to the Privacy Act, 5 U.S.C. § 552a(b); and
4. The sharing of PII to third parties must be consistent with Department policy, including DHS's privacy policies¹³ and information-sharing policies;¹⁴ and
5. Sharing must be consistent with all Component policies. For example, Component Privacy Officers should evaluate any proposed instances of sharing SPII with third parties to assess whether the sharing is authorized, and if a new or updated Privacy Notice is required.

Refer External Requests for Sensitive PII

- ⇒ From the public to your FOIA Officer
- ⇒ From the media to your Office of Public Affairs
- ⇒ From Congress to your Office of Legislative Affairs
- ⇒ From law enforcement to your Component Privacy Officer or PPOC and Chief Counsel
- ⇒ From other U.S. and foreign government agencies to your Component Privacy Officer or PPOC.

12. All DHS SORNs are posted on the DHS Privacy Office website (www.dhs.gov/privacy).

13. See, e.g., DHS Directive 047-01, Privacy Policy and Compliance [with associated DHS Instruction 047-01-001, Privacy Policy and Compliance]; DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information* (April 27, 2017); DHS Privacy and Civil Liberties Policy Guidance Memorandum 2009-01/Privacy Policy Directive 262-11, *The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy*.

14. See, e.g., DHS Directive 262-03, *DHS Information Sharing Environment Technology Program* [with associated DHS Instruction 262-03-001, *Implementing the DHS Information Sharing Technology Program*]; DHS Directive 103-01, *Enterprise Data Management Policy*; DHS Directive 262-05, *Information Sharing and Safeguarding* [see associated Instructions at <http://dhsconnect.dhs.gov/policies/Pages/directives.aspx>]; DHS Directive 262-07, *Disclosure of Homeland Security Information*.

Unauthorized Dissemination of SPII

Social Engineering

Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Please be wary of callers posing as authorized users, Help Desk representatives, or senior officials, asking for personal information or assistance to access DHS information or IT systems. Do not give sensitive information to anyone until you have confirmed their identity¹⁵ and that they have an official need to know.

Phishing

Phishing is a technical form of social engineering that uses email or malicious websites to elicit personal information by posing as a trustworthy individual or organization. Be suspicious of emails from unknown senders that solicit personal information or direct you to a website that requests personal information.

To counter these attacks, follow these anti-phishing practices:

- Exercise caution when asked for information – personal or professional – through emails, websites, social media interactions, and even phone calls.
- Never enter SPII in a pop-up window.
- Avoid clicking on hyperlinks in emails or on websites, if possible.

Forward all suspicious emails to DHSSPAM@hq.dhs.gov, or your Component spam email box.

Best Practices

Minimize Dissemination of SPII

Whenever possible, minimize the duplication and dissemination of electronic files and papers containing SPII.

- Only print, extract, or copy SPII when there are no other means of disseminating the data.
- Before emailing, printing, or copying, redact SPII that is beyond the scope of the data request or is not appropriate for the requestor to have.
- In some instances, it may be appropriate to create new spreadsheets or databases that contain SPII from a larger file or database. Before doing so, consult Attachment S1 in the DHS Sensitive Systems Policy Directive 4300A: *DHS Policy and Procedures for Managing Computer-Readable Extracts (CRE) Containing Sensitive PII*, which can be found on [DHS Connect](#). This document outlines DHS policies on how to manage computer readable extracts containing SPII.¹⁶
- Unauthorized replication or commingling of records may constitute an unauthorized or illegal Privacy Act system of records. Your Component Privacy Officer or PPOC should be consulted to provide guidance specific to the situation.
- **Social Media:** The Department engages in the operational use of social media¹⁷ only as authorized by DHS privacy policy, privacy laws applicable to DHS, applicable Federal

15. The OCSO recommends the following methods to confirm identity: (1) ask for their government identification card; (2) check their name in the government email address (GAL); or (3) ask your security officer; they can check with personnel security.

Government-wide policies, and other applicable statutory authorities. Consult [DHS Privacy Policy Instruction 110-01-001 for the Operational Use of Social Media](#), and your Component Office of Public Affairs, Privacy Officer or PPOC for additional guidance.

Email

Internally

- Although DHS policy permits emailing SPII within the DHS network without encryption or password-protection to a recipient with an official need to know, some Components do require encryption or password-protection. The DHS Privacy Office strongly recommends that you redact, password-protect, or encrypt SPII emailed internally.¹⁸ Use particular caution when emailing SPII to distribution lists.

Externally [beyond the DHS.gov domain/network]

- Never email SPII to or from a personal email account. Use of personal email accounts over DHS furnished equipment or network connections or to perform government business requires the approval of the DHS Under Secretary for Management (USM).¹⁹ Email SPII externally only within an encrypted or password-protected attachment using WinZip or Adobe Acrobat,²⁰ and provide the password separately by phone or email. Send only to individuals with an official need to know.
- Note: If someone outside of DHS sends you SPII in an unprotected manner, you must protect that data in the same manner as all SPII you handle once you receive it.
 - ⇒ For example, if someone outside of DHS sends you unsecured SPII in the body of an email, you must delete the SPII from the body of the email, put it in a separate attachment, and encrypt or password-protect the data if you wish to respond to that individual or email it to another recipient outside the dhs.gov domain. Alternatively, you can redact the SPII before responding to or forwarding the email.

16. The Chief Human Capital Office's (CHCO) Lockbox process is a best practice for the safe handling of non-routine or ad hoc CREs. Contact CHCO for the Lockbox Standard Operating Procedure.

17. "Operational use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings.

18. More information on the standards and use of encryption within the Federal Government and DHS can be found in the Department of Commerce's National Institute of Standards and Technology (NIST) (<https://www.nist.gov/>), including the following publications: NIST Special Publication 800-53, "Security Controls and Assessment Procedures for Federal Information Systems and Organizations"; NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"; and Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements for Cryptographic Modules."

19. Sending email to a personal account can trigger numerous vulnerabilities. See DHS Sensitive Systems Policy Directive 4300A, version 13.1, July 27, 2017. However, in some cases, it may be necessary to do so, for example, when CHCO communicates with job applicants.

20. For instructions on how to encrypt documents with WinZip or Adobe Acrobat Editor, consult your Help Desk. Note that OMB Circular A-130 requires the use of encryption for all Sensitive Information (FIPS 199 moderate- or high-impact) at rest and *in transit*. DHS is currently working to implement Public Key Infrastructure encryption for emailing Sensitive Information both internally and externally in HQ and all Components.

Mail²¹

Internally

- SPII should be sent in accordance with your Component's inter-office mail procedures or by DHS courier. Consult your supervisor for your office's accountable inter-office mail procedures. Confirm that the intended recipient received the information.

Externally

- For mailings containing a small amount of SPII (such as individual employee actions):
 - ⇒ Seal SPII materials in an opaque envelope or container and mail it using First Class Mail, Priority Mail, or a traceable commercial delivery service (e.g., UPS, FedEx).
 - ⇒ Never place SPII on an address label, mailing address, package, box, etc.
- For large data extracts, database transfers, backup tape transfers, or similar collections of SPII:
 - ⇒ Encrypt the data (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.

Equipment

- Avoid sending SPII using a fax machine unless you can confirm the fax will be received by the intended recipient. If possible, scan, encrypt, or password-protect the document, and email it instead.
- DHS staff are prohibited from using any non-government-issued removable media (such as USB drives), or from connecting such devices to DHS equipment or networks, or to store sensitive information on such devices. Some Components prohibit the use of all USB drives. Contact your Component Privacy Officer for guidance.



21. Components should follow the procedures established by [DHS Management Directive \(MD\) 11042.1, Safeguarding Sensitive But Unclassified \(For Official Use Only\) Information](#), for the transportation or mailing of backup media.

Disposing of Sensitive PII

You should periodically review the hard copy and electronic SPII in your possession to determine if it is still needed, especially prior to an office move or when leaving the agency. SPII, including that found in archived emails, must be disposed of when no longer required, consistent with the applicable NARA-approved records retention schedule,²² or as identified in the applicable SORN or PIA published on www.dhs.gov/privacy, in a manner that prevents loss, theft, misuse, or unauthorized access. In addition, you should determine whether the SPII is subject to a litigation hold or FOIA request before determining the appropriate course of action.²³

For questions about records retention schedules, contact your Component Records Officer, or email DHSRecordsManagement@hq.dhs.gov.

If destruction is required, take the following steps:

- Printed material must be destroyed using an approved cross-cut shredder or burn bag, or secured in a locked and properly-marked bin.
 - ⇒ Be especially alert during office moves and times of transition when large numbers of records are at risk.
- PEDs containing SPII must be sanitized according to your Information Security System Manager's standards when no longer needed.
- Retention of data in SharePoint must be consistent with the applicable records retention schedule for the original data collection.

If you are leaving the agency and determine that the SPII in your possession should not be destroyed, ask your supervisor to transfer it to a trusted DHS employee who either has an official need to know the SPII for official purposes, or who can secure it upon your departure. Follow the instructions in the factsheet, *How to Safeguard PII When Leaving DHS*, to properly secure, transfer, or destroy any SPII you may have stored in paper or electronic form during your tenure. Do not leave any SPII unattended in the office space you are vacating.

22. A records schedule provides mandatory instructions for the disposition of the records (including the transfer of permanent records and disposal of temporary records) when they are no longer needed by the agency. As part of the ongoing records life cycle, disposition should occur in the normal course of agency business. All Federal records must be scheduled (6 C.F.R. Part 1225) either by an agency schedule or a General Records Schedule (GRS).

23. To make this determination, contact your Component FOIA Officer or General Counsel.

Reporting a Privacy Incident

You must report all privacy incidents, whether suspected or confirmed, immediately to your Component Help Desk, Security Operations Center (SOC), Privacy Officer, or PPOC.

- For privacy incident response Points of Contact in every Component, please refer to Appendix A of the *Privacy Incident Handling Guidance*, listed in the Authorities section.
- Respond promptly to any requests about a privacy incident from your Component Help Desk, SOC, or Privacy Office.
- Document or maintain records of information and actions relevant to the privacy incident, as they may be required to investigate and remediate the incident.

Any alleged violations that may constitute criminal misconduct, identity theft, or other serious misconduct, or reflect systemic violations within the Department, will be reported to the DHS Office of the Inspector General (OIG) by the appropriate individuals as part of the privacy incident reporting and investigation process.

For more information on privacy incident reporting and handling, consult:

- DHS's *Privacy Incident Handling Guidance*, listed in the Authorities section;
- specific Component guidance; and
- DHS Privacy Policy Instruction 047-01-006, *Privacy Incident Responsibilities and Breach Response Team*, listed in the Authorities section.



Resources

⇒ **Factsheets:**

- *How to Safeguard Sensitive PII*
- *How to Safeguard Sensitive PII When Leaving DHS*
- *How to Prevent Online Harassment From “Doxxing”*

⇒ [DHS privacy policies](#)

⇒ [Federal Privacy Council](#) identity theft resources

⇒ [Identity Theft Resource Center](#)

⇒ US-CERT's [cyber tip sheets](#) offer advice on common security issues for non-technical computer users

