United States Department of the Interior

FISH AND WILDLIFE SERVICE
Washington, D.C. 20240

In Reply Refer To:
FWS/IRTM 045885

AUG 2 3 2010

Memorandum

To: Service Directorate

From: Acting Deputy Director

Subject: U.S. Fish and Wildlife Service (Service) Employee Responsibilities in Safeguarding Sensitive Personally Identifiable Information (PII)

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. The Service places a high priority on the protection of personal information we collect and/or maintain on individuals. All Service employees and contractors have a duty to protect PII in their custody from inadvertent or deliberate disclosure, modification, or destruction so that the security and confidentiality of the information is preserved.

PII is any information that can be used to distinguish or trace an individual's identity – such as name, Social Security Number (SSN), or biometric records – either alone or in combination with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name. This information may be on paper or in any other media format. Some PII is considered to be sensitive PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual and requires special protection. Some examples include, but are not limited to, the following:

- Social Security Number by itself
- Biometric identifier (such as fingerprints, iris scans, DNA) by itself
- An individual's name or an individual's unique identifier, in combination with one or more of the following elements:
  - Social Security Number (full or truncated(such as last 4 digits))
  - Driver's license number
  - Passport Number
  - Date of birth (month, day, and year)
  - System authentication information such as place of birth, mother's maiden name, account passwords or personal identification numbers, for systems containing sensitive PII
  - Unlisted home address or phone number
  - Financial/bank account number

- Personal or Government credit or debit card number
- Financial, medical or criminal record
- Employment information including ratings, disciplinary actions, performance elements, and standards.

Service employees are responsible for safeguarding all sensitive PII collected, maintained, and used by the Service. In the workplace, we are often responsible not only for our own personal information, but also for that of others. There are several things you can do to protect your privacy and the privacy of those whose personal information has been entrusted to the Service:

- Keep PII secure. When departing your area for lunch, meetings or at the end of the day; use a screen saver on your computer when you leave your desk, log off your computer at the end of the day, and lock up files containing sensitive PII when not under your direct control.
- Handle PII with care. Don't take sensitive PII outside of Service facilities except under approved telework arrangements or when approved by a supervisor to perform official Service duties. DOI Policy forbids the use of personally-owned information systems from accessing, storing, processing, or transmitting any sensitive PII on personally-owned information systems or electronic equipment such as personal computers/laptops or personal thumb drives.
- Dispose of PII properly. Dispose of sensitive PII using designated disposal bins (if available) or destroy using an approved method such as cross-cut shredding.
- Ensure the need to know. Before you provide sensitive PII to others, make sure you understand their need for it and how it will be protected.
- Think before you email. DO NOT send sensitive PII in an e-mail message or include as an attachment to an e-mail unless a valid encryption technology is installed on your work computer. Please see attached FAQ document for further information and clarification on valid e-mail encryption technology.
- Encrypt PII. Be careful when using portable storage devices; they can be easily lost or stolen. You MUST encrypt sensitive PII transmitted or downloaded and stored on approved portable storage devices; including laptops, memory sticks, disks, CDs, personal digital assistants (PDAs), and external hard drives. Please see attached FAQ document for further information on encryption software to use for safeguarding sensitive PII or contact your Regional IT Security Manager (RITSM).

Many Service employees and contractors have access to sensitive PII in the course of their work. Sometimes a "data breach" occurs related to such information. The term breach includes the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control over PII, and other conditions in which persons who are not authorized to access such information have access or potential access to it in usable form, whether physical or electronic. In accordance with the Office of Management and Budget (OMB) Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments Protection of Sensitive Agency Information," security incident involving the breach of PII must be reported to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery, whether suspected or confirmed breaches.

All security incidents involving the breach of sensitive PII, whether suspected or confirmed, must be reported immediately upon discovery to the Service's Enterprise Technical Support Help Desk by calling 800-520-2433 or by electronically submitting an Incident Response Form located at https://intranet.fws.gov/region9/irtm/bsm/sec_policies to the Service's Computer Security Incident Response Team (CSIRT). The Service's Enterprise Technical Support Help Desk will notify the Service CSIRT for further action and follow up as necessary. Do not hesitate to report a data breach even if you believe the incident is limited, small, or insignificant. The Service CSIRT experts will determine when an incident or breach needs additional focus and attention.

There are consequences, ranging from administrative to criminal, should an employee fail to handle PII appropriately. The particular facts and circumstances, including whether the breach was intentional, will be considered in taking appropriate action. The consequences for intentional and willful violations are defined in the Privacy Act of 1974 as amended (5 U.S.C. 552a). Additionally, DOI has issued the Privacy Loss Mitigation Strategy policy, which includes Rules and Consequences for failing to comply with DOI's privacy policies and procedures or with the requirements of federal privacy regulations (see Section 3.2).

A list of frequently asked questions concerning the responsibilities of all Service employees and contractors when handling PII is attached to this bulletin for further clarification. For additional guidance or questions related to the proper handling of PII, please contact Teresa Fryer, the Service's Bureau Chief Information Security Officer/Privacy Program Manager, at Teresa_fryer@fws.gov or by calling 703-358-1823. For information security requirements related to handling PII, please contact your RITSM. A list of the RITSMs can be found at https://intranet.fws.gov/region9/irtm/bsm/sec_contacts/contacts_iitsm.php.

Attachment

Personally Identifiable Information (PII) Frequently Asked Questions

This Frequently Asked Questions (FAQ) document will discuss topics pertaining to FWS employee and contractor responsibilities regarding the handling of sensitive Personally Identifiable Information (PII).

GENERAL

1. What is the definition of sensitive Personally Identifiable Information (PII)?

PII is any information that can be used to distinguish or trace an individual's identity – such as name, Social Security Number (SSN), or biometric records – either alone or in combination with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name. This information may be on paper or in any other media format. Some information that is considered to be PII is available in public sources such as telephone books, public websites, university listings, etc. This type of information is considered to be public PII. See FAQ #4 below for examples of public PII. In contrast, some PII is considered to be sensitive PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual and requires special protection. See FAQ #5 for examples of sensitive PII.

2. What does it mean when information can be traced or is traceable to an individual?

When information is traceable to an individual, the personal identity of an individual can be deduced from a combination of information. For example, anonymous, unencrypted medical records indicating an individual's diagnosis with clinical depression are accessed. These records are combined with the unit's posted work schedule indicating that Joe is busy from 2 – 4 pm every Wednesday, and also with the company's health clinic schedule which offers a depression clinic every Wednesday from 2 – 4 pm. Thus, it can be deduced that Joe is the individual who is clinically depressed. The medical records should have been properly encrypted in this case.

3. Who should I contact if I have any questions regarding PII?

For additional guidance or questions related to PII, contact the FWS Privacy Program Manager, Teresa Fryer, at Teresa_fryer@fws.gov or by calling 703-358-1823.

4. What is considered Public PII?

Public PII refers to information about an individual that is publicly available. However, if any of the information below is combined with Sensitive PII listed in FAQ #5 below, this information would become Sensitive PII. The following information is considered Public PII:

- An individual's name by itself
- Work telephone number

- Work cell phone number
- Work pager number
- Work fax number
- Work email address
- Work location or facility
- Publicly listed home email address
- Publicly listed home telephone number
- Publicly listed home address
- Educational Transcripts, unless they include information that would be considered sensitive PII
- Written biographies
- Resumes, unless they include information that would be considered sensitive PII

5. What information is considered Sensitive PII?

Sensitive PII is any information maintained by FWS that can be used to uniquely identify an individual, including, but not limited to:

- Social Security Number by itself
- Biometric identifier (such as fingerprints, iris scans, DNA) by itself
- An individual's name or an individual's unique identifier, in combination with one or more of the following elements:
    - Social Security Number (full or truncated(such as last 4 digits))
    - Driver's license number
    - Passport Number
    - Date of birth (month, day, and year)
    - System authentication information such as place of birth, mother's maiden name, account passwords or personal identification numbers, for systems containing sensitive PII
    - Unlisted home address or phone number
    - Financial/bank account number
    - Personal or Government credit or debit card number
    - Financial, medical or criminal record
    - Employment information including ratings, disciplinary actions, performance elements, and standards.

For questions on other data elements not indicated on this list, you should contact the FWS Privacy Program Manager, Teresa Fryer, at Teresa_fryer@fws.gov or by calling 703-358-1823.

6. What is a PII Breach?

A PII breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users or for other-than-authorized purpose have access or potential access to PII, in usable form whether physical or electronic.

7. What should one do if an individual suspects a PII breach?

A breach, whether suspected or actual, involving sensitive PII, whether in physical (non-electronic) or electronic form, must be reported immediately upon discovery to the FWS Enterprise Technical Support Help Desk by calling 1-800-520-2433 or by electronically submitting an Incident Response Form located at https://intranet.fws.gov/region9/irtm/bsm/sec_policies to the FWS Computer Security Incident Response Team (CSIRT). The FWS Enterprise Technical Support Help Desk will notify the FWS CSIRT for further action and follow up as necessary. For additional guidance on reporting PII data breaches, contact the Regional Privacy Point of Contact if there is one assigned or the Regional IT Security Manager (RITSM). A list of RITSMs can be found at https://intranet.fws.gov/region9/irtm/bsm/sec_contacts/contacts_iitsm.php.

8. Where can I find additional guidance regarding protection of PII?

DOI specific privacy requirements and responsibilities can be found at http://www.doi.gov/ocio/privacy/index.html.

ENCRYPTION

9. When should PII be encrypted?

OMB Memorandum M-06-16 states that all sensitive PII data on mobile computers/devices, whether within or outside the Agency's physical environment, shall be encrypted. In addition, DOI Information Technology Security Policy Handbook 3.1, *AC-17 Remote Access and PII*, states sensitive PII data when transmitted and/or stored outside the Agency's secured physical perimeter, or when accessed remotely shall be encrypted using FIPS 140-2 validated encryption on all mobile media and devices (e.g., removable media, portable/mobile devices, remote workstations, etc.). However, industry security best practices advise the encryption of all sensitive PII, even when transmitted within the agency's secure network, as the potential exists for sensitive PII to be mistakenly forwarded outside the agency. In addition, FWS must comply with DOI Office of the Chief Information Officer (OCIO) guidelines specified in memorandum dated August 25, 2006 entitled *Protection of Personally Identifiable Information (PII) and Department Sensitive Information* and memorandum dated December 15, 2006 entitled *Additional Guidance for the Protection of Personally Identifiable Information (PII) and Department Sensitive Information.* Both of these memorandums can be found at http://www.myinterior.doi.net/ocio_memorandums.html.

10. How do I encrypt files containing sensitive PII on removable media and portable storage devices, including laptops, PDAs, external hard drives, etc.?

In a memorandum from the Director, FWS dated October 15, 2007; FWS had selected three options to implement encryption on mobile devices. These options, along with

additional technical requirements and information, can be viewed and downloaded from https://intranet.fws.gov/region9/irtm/bsm/info_assurance/encrypt.php.
Additionally, the FWS Data at Rest (DAR) project team is currently implementing the Department's DAR solution using McAfee Endpoint Encryption Software on new laptops. For further information on encrypting sensitive PII on removable media and portable devices, please contact your Regional Chief Technology Officer (CTO). A list of Regional CTOs can be found at https://intranet.fws.gov/region9/irtm/ctocontact.html.

11. If a file or device containing sensitive PII is password protected, is this the same as being encrypted?

No. Password protected files or devices do not meet the requirements of encrypting sensitive PII.

12. How do I encrypt sensitive PII on a thumb drive?

Thumb drives used for downloading and storing sensitive PII must use FIPS 140-2 validated encryption in accordance with Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, and must be approved by the Regional CTO. DOI Policy forbids the use of personally-owned thumb drives for storing sensitive PII. For more information on approved thumb drives, please contact your Regional CTO. A list of Regional CTOs can be found at https://intranet.fws.gov/region9/irtm/ctocontact.html.

13. How do I encrypt sensitive PII in an e-mail message?

Sensitive PII, whether in the body of an e-mail or as an attachment must be encrypted using a valid e-mail encryption technology, either Lotus Notes or Outlook Exchange (whichever client is being used). As long as both the sender and receiver are using the same e-mail client (Lotus Notes or Outlook Exchange, whichever is being used) and they are within the same agency, the e-mail encryption technology may be used. However, if sending an encrypted e-mail message to a user outside the Bureau (non-DOI user) and they do not have Lotus Notes or Outlook Exchange (whichever client is being used), the e-mail encryption technology will not work. DOI is working to obtain an enterprise level solution; however, FWS is currently working on a solution using existing internal resources and will provide additional information to employees at a future date. Remember that an e-mail message must be encrypted each and every time it is sent or forwarded. For further information on encrypting sensitive PII in e-mail messages contact the FWS Enterprise Technical Support Help Desk at 1-800-520-2433.

14. How do I encrypt protected PII on a BlackBerry?

All settings and configurations (including security settings) on FWS BlackBerry devices are controlled by the Blackberry Enterprise Server (BES). The BES servers have been configured to enable "content protection" on all Blackberry devices that communicate

with the BES servers. Content protection encrypts data stored locally on the device, for example, emails, Internet browser cache and address book entries/contacts.

15. If a SSN is known to be valid, but not included with the individual's name or other information, is it, by itself, considered sensitive PII and, therefore, needs to be encrypted?

Yes. An individual's SSN alone is considered Sensitive PII even if it is not associated with a specific individual. For example, a list of employees SSNs is Sensitive PII and must be protected as such, including encryption for electronic transmission.

16. When public PII (see FAQ #4 above) is combined with sensitive PII (see #5 above), is it required to be encrypted?

Yes. If public PII is combined with sensitive PII, the information must be encrypted.