NOAA Privacy Training –February 2016

NOAA NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
UNITED STATES DEPARTMENT OF COMMERCE

Presenters:

Mark H. Graff, Esq.
Bureau Chief Privacy Officer (BCPO)
Office of the Chief Information Officer
National Oceanic and Atmospheric Administration
Mark.graff@noaa.gov

Sarah Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer
Office of the Chief Information Officer
National Oceanic and Atmospheric Administration
Sarah.brabson@noaa.gov

How to Protect Personally Identifiable Information (PII) and Business Identifiable Information (BII)

Presented: April 6, 2016

Training Goals & Objectives

- Understand your role in privacy
- Be familiar with relevant privacy laws and OMB guidance
- Understand Department of Commerce (the Department) policy on electronic transmission of PII
- Understand how to properly handle PII and BII within NOAA
  - How to distinguish between Sensitive and Non-Sensitive PII
  - How to use the Accellion Secure File Transfer tool to encrypt PII

Privacy Protections

- When the Department collects personal information, it has a duty and responsibility to protect that information from misuse.
- Privacy protection includes the protection of personal privacy rights of individuals from unauthorized collection, maintenance, use, and disclosure
- Business identifiable information (BII) received by the Department must be similarly protected, in accordance with applicable laws.

Your Role in Privacy

- **As a NOAA employee, you are responsible and accountable for**
  - knowing what constitutes personal information and business identifiable information;
  - handling personal and business identifiable information;
  - protecting personal and business identifiable information; and
  - following all laws, rules, regulations, and Department as well as Bureau policies and procedures regarding personal and business identifiable information.

Key Privacy Laws

- Privacy Act of 1974 (PA) (5 U.S.C. 552a)
- Freedom of Information Act (FOIA) (5 U.S.C. 552)
- E-Government Act of 2002
- Federal Information Security Management Act (FISMA) (44 U.S.C. § 3541)
- Trade Secrets Act (18 USC 1905)
- Additional privacy laws regulate other areas, such as government access to bank and other financial records, identity theft, trade secrets, health records, and education records.
- OMB Memoranda – see next page

Other Guidance

- **OMB Memoranda**
  - **M-03-22** Guidance for Implementing the Privacy Provisions of the E-Gov Act,
  - **M-06-15** Safeguarding Personally Identifiable Information (PII)
  - **M-06-16** Protection of Sensitive Agency Information
  - **M-06-19** Reporting Incidents Involving Personally Identifiable Information
  - **M-07-16** Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)

Other Guidance, continued

- **OMB Memoranda continued**
  - **M-10-23** Guidance for Agency Use of Third-Party Websites and Applications
  - **M-11-02** Sharing Data While Protecting Privacy
  - **M-16-3,** Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
  - **M-16-4**, Cybersecurity and Strategy and Implementation Plan (CSIP) for the Federal Civilian Government.

- **Department of Commerce IT Privacy Policy**

DOC Policy on Electronic Transfer of Sensitive PII

Department policy states that if sensitive PII must be electronically transmitted, then it must be protected by secure methodologies such as encryption**, Public Key Infrastructure (PKI)**, or **secure sockets layer (SSL)**.

Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules", provides the standard to which encryption methodologies must conform.

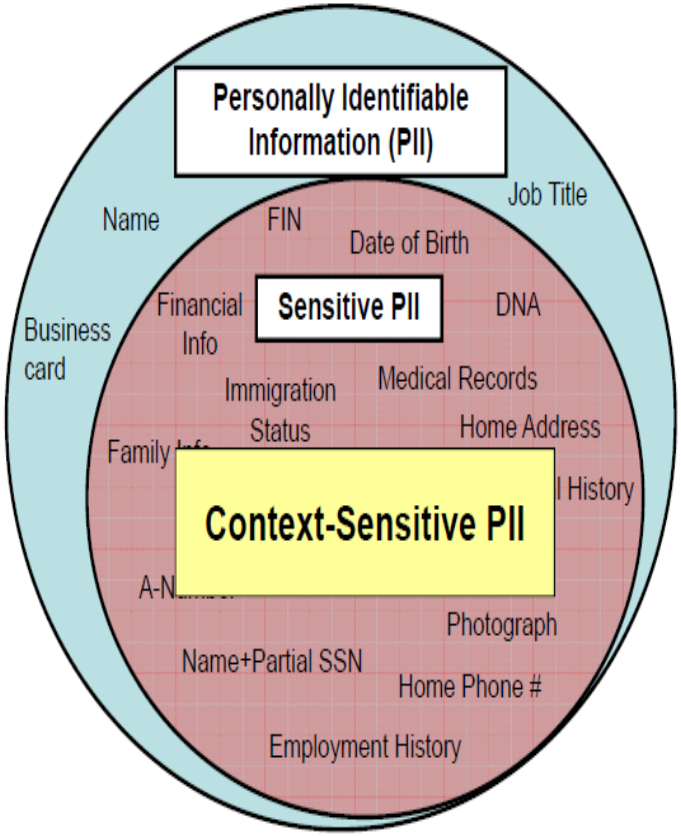
The transmission of sensitive PII, even if it is protected by secure means, must be kept to a minimum.

Defining PII

- Personally identifiable information (PII) is not always easy to recognize. OMB has defined PII as
  - *"information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."*

Examples of PII

- Social security numbers (SSNs)
- Place of birth
- Date of birth
- Mother's maiden name
- Biometric information
- Medical information
- Personal financial information
- Credit card or purchase card account numbers
- Passport numbers
- Criminal history



PII vs. Sensitive PII

Personally Identifiable Information (PII)

- Any information that permits the identity of an individual to be inferred directly or indirectly

Sensitive PII

- PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual.
- SSN, date of birth, etc.
- Medical, criminal, employment information
- Biometric information, such as fingerprints

* Context can make otherwise ordinary PII sensitive

Social Security Numbers are Sensitive PII

- SSNs including truncated SSNs revealing only the last four digits, are considered sensitive PII, both stand-alone and when associated with any other identifiable information. If it is determined that electronic transmission is required, then secure methods must be employed.

Identifying PII

- When deciding whether PII is sensitive or non-sensitive, it is important to consider the following factors:
  - The types of information
  - The context of the information
  - Obligations or expectations regarding the protection of the information
  - Risk (probability and consequences) of loss or compromise of the information
  - **Context** is particularly important. The same types of information can be sensitive or non-sensitive depending upon the context. For example, a list of names and phone numbers for the Department softball roster is very different from a list of names and phone numbers for individuals being treated for an infectious disease.
  - It is important to use good judgment when deciding whether PII is sensitive or non-sensitive. When in doubt, treat PII as sensitive!

Defining BII

- Department policy states that
  - business identifiable information (BII) consists of information that is defined in the FOIA as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."
- "Commercial" is not confined to records that reveal basic commercial operations but includes any records [or information] in which the submitter has a commercial interest, and may include information submitted by a nonprofit entity.

Identifying BII

- Other terms for business identifiable information that must be protected from disclosure are:
  - "confidential business information"
  - "confidential commercial information"
  - "proprietary information"

Examples of BII

- Financial information provided in response to requests for economic census data;
- Business plans and marketing data provided to participate in trade development events;
- Commercial and financial information collected as part of export enforcement actions;
- Proprietary information provided in support of a grant application or related to a federal acquisition action;
- Financial records collected as part of an investigation.

Digital Do's and Don'ts

- **Do's**
  - Store PII on Government Systems Only
  - Encrypt sensitive PII in emails and on Mobile Computers, Media (e.g., CDs, DVDs, USB drives), and Devices (e.g., laptop computers, hard drives)
  - Regularly review your PII holdings to ensure you still need it for your work
  - Log off or lock your computer system when leaving it unattended.
  - Use appropriate methods for destroying sensitive paper PII (e.g., shredding, using a burn bag) and securely deleting sensitive electronic PII (e.g., empty the Windows "recycle bin")
- **Don'ts**
  - Email unencrypted sensitive PII
  - Access PII from public (non-Department) computers, such as those in hotels or business centers
  - Keep PII, either paper or electronic, that you don't need or that have passed their retention schedules
  - Share your passwords, credentials, or Personal Identification Numbers (PINs) with anyone.
  - Throw paper containing sensitive PII or media containing unencrypted sensitive PII (e.g., CD, DVD) into a regular waste bin

Additional Rules for Communicating, Sending, and Receiving PII

- **FIRST and FOREMOST -** Do Not distribute or release PII to other employees or individuals unless it is within the scope of their official duties and they have a need to know, and redact sensitive information not needed by the recipient
- **EMAIL**: When emailing sensitive PII, send it within an encrypted attachment.
- **FAX:** When faxing information, include an advisory statement about the contents on the cover sheet and notify the recipient before and after transmission.
- **HARD COPY**: Do not leave sensitive PII unattended on printers, fax machines, or copiers.

Additional Rules for Communicating, Sending, and Receiving PII

- **MAILING**: Physically secure sensitive PII when in transit. Do not mail, or send by courier sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted. Seal sensitive PII in an opaque envelope or container, and mail using First Class or Priority Mail, or a commercial delivery service (e.g., DHL or FedEx).

Additional Rules for Communicating, Sending, and Receiving PII

- **MOBILE DEVICES:** Sensitive PII may be saved, stored, or hosted only on Department-authorized equipment (including contractor-owned equipment or a system that is approved to be used as a government system). Personally owned computers may not be used to save, store, or host sensitive PII that is collected or maintained by the Department.
- **SHARED DRIVES**: 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. Password-protect both the document and the folder you save it to.

Consequences of PII Loss

Consequences to an Individual:

- Identity Theft
- Embarrassment
- Blackmail
- Discrimination

Consequences to an Organization

- Loss of public trust
- Legal liability
- Remedial costs (e.g., paying for credit monitoring systems)
- Administrative burden
- Embarrassment (front page news story)

Defining a PII Incident

- A PII incident is 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 other than authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic [OMB M-07-16].

Identifying a PII Incident

Confirmed *OR* **Suspected**

Loss *OR* **Compromise**

OF

SENSITIVE PII

Examples of Reportable PII Incidents

- Sensitive PII that is emailed, internally or externally, that is not encrypted
- Sensitive PII left in a public area, such as on or near a copy machine or in an open waste bin
- Lost or stolen USB drive or a CD
- Sensitive PII lost in the mail
- Lost or stolen laptop
- Lost or stolen smart phone
- Lost or stolen briefcase containing sensitive paper-based PII
- Sensitive PII shared with individuals who do not have a need to know

Reporting Lost PII is Your Responsibility!

- **IMMEDIATELY report ALL known or suspected losses of PII to both your supervisor AND your bureau Computer Incident Response Team (CIRT)!**
  - **Provide as much information as possible, including:**
    - Your name and contact information
    - Description of the incident
    - Where the incident occurred
    - What type of media or device was involved
    - Date and time the incident occurred
    - Any controls enabled to mitigate the loss
    - Number of individuals potentially affected
  - **Report the incident immediately, even if you do not have all of the information.**

Reporting PII Incidents

- Report to N-CIRT directly for all PII incidents.
  - N-CIRT

    ncirt@noaa.gov

    301-713-9111

    https://www.csp.noaa.gov/V3_Form/authenticated-form/cc-email.php/
- If you become aware of a PII incident outside of NOAA within DOC report it to the appropriate bureau POC:

- **BEA CIRT**

  helpdesk@bea.gov

  202-606-5353
- **BOC CIRT**

  boc.cirt@census.gov

  301-763-5141 or 1-877-343-2010 (for PII breaches that occur after hours)
- **ITA CIRT**

  OCIO.CustomerSupport@mail.doc.gov

  202-482-1955 or 202-482-4641 or 877-206-0645 (toll free)
- **NIST CIRT**

  siirt@nist.gov

  301-975-2000
- **NOAA CIRT**

  ncirt@noaa.gov

  301-713-9111
- **NTIS CIRT**

  security@ntis.gov

  703-605-6440 or 703-389-1553
- **USPTO CIRT**

  cirt@uspto.gov

  571-272-6700

Privacy is everyone's responsibility!

Remember:

- YOU are critical to ensuring PII protection.
- YOU must recognize what constitutes PII.
- YOU must safeguard PII appropriately.
- YOU must seek help/advice when you are unsure.

Securely Transferring PII

I must send PII as part of my regular duties.

- How PII be properly transmitted?
  - Using Secure File Transfer
  - Enabling 2SV and using Google Apps **only within the NOAA.gov Domain**
- This portion of the presentation will be given by our OCIO, Cyber Security Division (CSD)

DOC Policy: Electronic Transfer of PII

At Commerce, BII is afforded the same protection as PII and must be similarly protected, in accordance with applicable laws.

Commerce policy states that if sensitive PII must be electronically transmitted, then it must be protected by secure methodologies such as encryption, Public Key Infrastructure (PKI), or secure sockets layer (SSL). Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, provides the standard to which encryption methodologies must conform.

The following types of PII are considered sensitive when associated with an individual, and secure methods must be employed when transmitting this data:

- Social Security Number (SSN)
- Place of birth
- Date of birth
- Mother's maiden name
- Biometric information
- Medical information, except brief references to absences from work
- Personal financial information
- Credit card or purchase card account numbers
- Passport numbers
- Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and results of background investigations
- Criminal history
- Any information that may stigmatize or adversely affect an individual

Social Security Numbers (SSNs), including truncated SSNs revealing only the last four digits, are considered sensitive PII, both standalone and when associated with any other identifiable information. If it is determined that electronic transmission is required, then secure methods must be employed.

The transmission of sensitive PII, even if it is protected by secure means, must be kept to a minimum. Non-sensitive PII may be transmitted in an unprotected form.

This policy applies to Commerce employees, contractors, interns, guest researchers, foreign nationals, and others who are authorized to use Commerce resources.

DOC User
Accellion Secure File Transfer (SFT)

To send encrypted files, you must have an Accellion account.

To register with the Secure File Transfer Web Application:

1. In your web browser, go to https://sft2.doc.gov/
2. Click on "I don't have an account yet."
3. Enter your Department of Commerce email address and click "register."
4. Wait for the verification code to be emailed to you. Once you have received the email, verify your email address using the link provided and assign yourself a password.
5. Once registered, return to https://sft2.doc.gov/ to send files.

To support the demand of the Accellion Secure File Transfer solution, license provisioning has been put in place. Licenses are being provisioned as a user signs up and requires the service. **After 30 days of inactivity, the license will be re-provisioned (account deactivated) so it frees up a license for another user.**

Once the account is re-provisioned, it no longer exists and the user will be required to go through the registration process to utilize the service again. Note: recipient-only accounts are not subject to this deactivation.

How to Instruct Non-DOC Partner(s) to Send Secure Files

Step 1: Invite External Partner to Send File

- DOC team member logs into Accellion.
- Click "Invite User" button located in the right hand corner on the Send File tab.

Step 2: Send External Partner Invite

- Type the external partner's email address in the email box. Use a comma to separate more than one email address. Type any desired note in the "Add an optional note" box, which will display in the body of their email when they receive the invitation.

Step 3: External Partner Uses Invite

- The external partner will receive an email to send a file to a DOC team member.
- To accept the invitation to send the file, the external partner clicks on the web link contained in the invite email.

Step 4: External Partner Creates Account

- The main Accellion page will be displayed. Create a password at least 12 characters in length and validate it. Once complete, click "Register" then click "Ok."

Step 5: External Partner Sends File

- The external partner can now send files to a DOC team member. Note: Files can only be sent to the DOC team member that invited the external partner.
- Use "Choose File Folder" to upload files and open space for body of email text. Note: Body of email is not encrypted.
- Press "Send" when complete.

Accellion Secure File Transfer

Need help or have more questions about using Accellion Secure File Transfer?

E-mail: AccellionAlerts@doc.gov


NOAA
NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE

Questions

Additional Information

Best Practices

- Any email messages that contain PII must be **ENCRYPTED!**
- Any PII that is contained or maintained on “mobile” equipment (Laptop, IPAD, PDAs, memory sticks etc.) must be **ENCRYPTED!**

Best Practices

- **Think PRIVACY** when considering the PII that you store on your computer, memory stick, PDA, etc.
- **Think PRIVACY** when you send/receive e-mails no unencrypted emails containing PII
- **Think PRIVACY** use only approved encryption methods for transmitting PII
- **Think PRIVACY** Any misuse or unauthorized access may result in both civil and criminal penalties."

Best Practices

- **Think PRIVACY** when you create documents--do you need to include the SSN?
- **Think PRIVACY** when placing documents in public folders in Outlook and on public web sites.
- **Think PRIVACY** when disposing of PII--use cross-cut shredding, if possible

Your Responsibilities

- **Do NOT** collect personal data without authorization.
- **Do NOT** distribute or release personal information to other employees unless they have an official need-to-know.
- **Do NOT** be afraid to challenge anyone who asks to see PA information.
- **Do NOT** maintain records longer than permitted.
- **Do NOT** destroy records before disposal requirements are met.
- **Do NOT** place unauthorized documents in PA systems of records.

Your Responsibilities

- **Do NOT** co-mingle information about different individuals in the same file.
- **Do NOT** use interoffice envelopes to mail Privacy data.
- **Do NOT** place privacy data on shared drives, multi-access calendars, the Intra or Internet that can be accessed by individuals **who do not have an official need-to-know**.
- **Do NOT** hesitate to offer recommendations on how to better manage Privacy data.

Privacy Program Metrics on PII incidents

Number of Open Incidents by Cause