Key Privacy Laws and Other Guidance

The Department of Commerce adheres to federal privacy laws and guidance to ensure that the collection, use, and maintenance of sensitive information, such as personally identifiable information and business identifiable information, is properly safeguarded.

Privacy Regulations:

- Freedom of Information Act (FOIA) – 5 U.S.C. § 552
- Privacy Act of 1974 – 5 U.S.C. § 552a
- The E-Government Act of 2002
- Trade Secrets Act – 18 U.S.C. § 1905
- Federal Information Security Management Act (FISMA) of 2002 – 44 U.S.C. § 3541
- Paperwork Reduction Act of 1995 (PRA)

Guidance:

- OMB Memorandums
  M-03-22 , M-06-15, M-06-16,
  M-06-19, M-07-16, M-10-23
- Department of Commerce IT Privacy Policy

The Office of Privacy and Open Government (OPOG) is part of the Office of the Chief Financial Officer and Assistant Secretary for Administration (CFO/ASA) and reports to the Deputy Assistant Secretary for Administration. The CFO/ASA's authority is delegated through Department Organization Order 20 -31, Chief Privacy Officer and Director of Open Government.

OPOG's functions include:

- Privacy
- Open Government
- Freedom of Information Act (FOIA)
- Directives Management
- Federal Advisory Committees

Senior Leadership:

- Dr. Catrina D. Purvis, Esq.
  Senior Agency Official for Privacy, Chief Privacy Officer and Director of Open Government
- Lisa J. Martin
  Deputy for Departmental Privacy Operations
- Joey Hutcherson, TPM, PMP, CIPP/G
  Deputy for Open Government
  and Office of the Secretary Privacy Operations
- Michael J. Toland
  Deputy for FOIA and Privacy Act Operations

http://www.osec.doc.gov/opog/

Office of Privacy & Open Government

Privacy Program

How to PROTECT Personally Identifiable Information (PII) and Business Identifiable Information (BII) when transmitting to AUTHORIZED USERS using

ACCELLION

Secure File Transfer

Personally Identifiable Information (PII). The term "PII," as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Business Identifiable Information (BII) consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)).

The Office of Privacy and Open Government (OPOG)

E-mail: cpo@doc.gov

DOC Policy: Electronic Transfer of PII

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.

Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained.

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

Examples of BII include:

- 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

If it is determined that electronic transmission is required, then secure methods must be employed. The transmission of sensitive PII and BII, 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.

Accellion Secure File Transfer

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

E-mail: AccellionAlerts@doc.gov