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 Modernization Act of 2014 - Public Law No. 113-283
- Paperwork Reduction Act of 1995 (PRA)

Guidance:

- OMB Memoranda & Circulars
  M-03-22, M-10-22, M-10-23, M-11-02, M-16-04, M-16-14, M-17-06, M-17-12, Circular A-108, Circular A-130
- 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)/Privacy Act (PA)
- Directives Management
- Federal Advisory Committees

Senior Leadership:

- Dr. Jennifer Goode
  Acting Senior Agency Official for Privacy, Chief Privacy Officer and Director of Open Government
- Tahira Murphy
  Acting Deputy Program Director for Departmental Privacy & OPOG Office Operations and Acting Deputy Program Director for Privacy Compliance
- Nicholas Cormier
  Deputy Chief FOIA Officer and Deputy Program Director for FOIA Operations

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

KITEWORKS
BY ACCELLION

Secure File Collaboration

Personally Identifiable Information (PII). The term "PII" 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

http://www.osec.doc.gov/opog/
https://www.commerce.gov/Privacy

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., performance ratings, leave balances, 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
Kiteworks Secure File Collaboration (SFC)

To send encrypted files, you must use Kiteworks SFC. Kiteworks SFC uses the Commerce Web Solutions Authenticator (Authenticator) account for authentication. DOC users will need to register and establish an Authenticator account to use Kiteworks SFC.

1. In your web browser, go to https://pass.commerce.gov and register your Authenticator account.
2. Click on the "Register/Password reset" link at the top of the login page to register a new Authenticator account or reset your password for an existing account.
3. Enter your DOC email address and click "Submit." (A token to be used to create your password (or reset your password) will be emailed to your DOC email address.).
4. Copy and paste the token from your email into the token form and click "Submit."
5. Your browser will then be redirected to the new password form. Enter a password, confirm it, check the box to acknowledge the DOC Rules of Behavior and click save. More information on registering for Authenticator is available on CommerceConnection.
6. Once your Authenticator account has been set up, go to https://sfc.doc.gov/ and enter your Department of Commerce email address and your Authenticator account password.
7. Once logged in, you may use the SFC to send and receive files securely.

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

Method 1: Copy External Partner on a Secure Email

- DOC team member logs into Kiteworks SFC and creates a secure email, including the external partner on the TO:, CC:, or BCC: lines.
- External partner receives the email and must create a Kiteworks account following instructions provided through a web link in the email.
- Once an account is created external partner logs in to review and respond, including sending secure files.

Method 2: Request Files from External Partner

- DOC team member logs into Kiteworks SFC and chooses "All Files."
- DOC team member chooses "..." and selects "Request Files" from drop down menu.
- Type the external partner's email address in the email box. Use a comma to separate more than one email address. Type any desired text in the email which will accompany the request. Please note the entire communication is encrypted.
- 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 and follows instructions for creating an account.
- Once registered, the external partner can send files to the original DOC requesting team member. As outlined above, the entire communication, including any text in notes or the email body, is encrypted.

Kiteworks Secure File Transfer

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

E-mail: itservicedesk@doc.gov