Commerce Privacy Mission Statement

The Department of Commerce (DOC) is committed to safeguarding personal privacy. Individual trust in the privacy and security of PII is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information-management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy considerations in all systems, programs, and policies.

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 Memorandums M-03-22, M-06-15, M-06-16, M-06-19, M-07-16, M-10-22, M-10-23, M-11-02, M-16-14, and M-17-06
- Department of Commerce IT Privacy Policy

Office of Privacy & Open Government

Privacy Program

Personally Identifiable Information (PII) Breach Incident Reporting

The Privacy Act of 1974, 5 U.S.C. § 552a (e)(10), and Office of Management and Budget Memorandum (OMB) M-07-16, Attachment 1 (A)(b) requires agencies to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Office of Privacy and Open Government

Email: cpo@doc.gov

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII), as defined in the Office of Management and Budget Memorandum 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.

The following types of PII are considered sensitive when associated with an individual: Social Security Number (including truncated form), place of birth, date of birth, mother's maiden name, biometric information, medical information (excluding 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, disciplinary actions, and results of background investigations), criminal history, and any information that may stigmatize or adversely affect an individual.

EMPLOYEE/CONTRACTOR RESPONSIBILITIES

As a Department of Commerce employee/contractor, you are responsible and accountable for:

- Knowing what constitutes PII
- Following Federal laws, rules, regulations, and Departmental privacy policy
- Taking steps to prevent a PII breach from occurring
- Recognizing a PII breach incident and immediately reporting it upon discovery/detection
- Successfully completing training relative to safeguarding PII

WAYS TO PROTECT PII

- Electronically transmit sensitive PII by secure methodologies, such as encryption, Public Key Infrastructure (PKI), or secure sockets layer (SSL).
- Encrypt sensitive PII on mobile computers, media (e.g., CDs, DVDs, USB drives), and devices (e.g., laptop computers, hard drives).
- Log off or lock your computer system when leaving it unattended.
- Destroy sensitive paper PII by shredding, using a burn bag, etc.
- Delete sensitive electronic PII by emptying the Windows "recycle bin."
- Store sensitive PII on Federal Government systems only.
- Clear your desk and ensure sensitive PII is properly secured while you are away and at the end of each day.

STEPS FOR REPORTING PII INCIDENTS

1. Upon discovery/detection, immediately report a suspected or confirmed PII breach incident to your supervisor/Contracting Officer's Representative (COR) and Bureau/Operating Unit (BOU) Computer Incident Response Team (CIRT).
2. Provide details of the PII breach incident (e.g., summary of incident including name(s) of individual(s) involved, date, time, and place incident occurred, type of PII involved, type of media or device involved, number of individuals potentially affected, any controls enabled to mitigate loss, etc.).
3. Maintain or document information and/or actions relevant to the PII breach incident.
4. Complete corrective/remedial actions, if appropriate.

COMMERCE OPERATING UNIT CIRT REPORTING OFFICES

Department of Commerce (DOC) CIRT
- doc-cirt@doc.gov
- (202) 482-4000
- https://connection.commerce.gov/overview/about-doc-cirt

PII incidents occurring in EDA, ESA, MBDA, NTIA, OIG, and OS shall be reported directly to DOC CIRT.

Bureau of Economic Analysis (BEA) CIRT
- helpdesk@bea.gov
- (301) 278-9407

Bureau of Industry and Security (BIS) IT Security
- BISITSecurity@bis.doc.gov
- (202) 482-0623 or (202) 482-1188

Bureau of the Census (BOC) CIRT
- boc.cirt@census.gov
- (301) 763-3333 or (877) 343-2010 (after hours)

International Trade Administration (ITA) CIRT
- CSC@trade.gov
- (202) 482-1955 or (877) 206-0645 (toll free)

National Institute of Standards and Technology (NIST) CIRT
- itac@nist.gov
- (301) 975-5375 (Gaithersburg, MD); (303) 497-5375 (Boulder, CO)

National Oceanic and Atmospheric Administration (NOAA) CIRT
- ncirt@noaa.gov
- (301) 713-9111

National Technical Information Service (NTIS) CIRT
- security@ntis.gov
- (703) 605-6321 or (703) 216-8054

U.S. Patent and Trademark Office (USPTO) CIRT
- CyberSecurityInvestigations@USPTO.GOV
- (571) 272-6700