DEPARTMENT OF COMMERCE

PRIVACY PROGRAM PLAN

SEPTEMBER 2017

Department of Commerce
Privacy Program Plan
Table of Contents

Department of Commerce Privacy Program Plan

1 Introduction

1.1 Purpose of the Privacy Program Plan

The purpose of the Department of Commerce (DOC or the Department) Privacy Program Plan is to provide an overview of the Department's privacy program. This plan highlights:

- A description of the structure of the privacy program;
- The resources dedicated to the privacy program;
- The role of the Senior Agency Official for Privacy (SAOP) and other privacy officials and staff;
- The strategic goals and objectives of the privacy program;
- The program management controls in place to meet applicable privacy requirements and manage privacy risks; and
- Any other information deemed necessary by the Department's privacy program.

1.2 DOC Privacy Website for Information

The Department's privacy website is located at www.commerce.gov/privacy. The website contains information such as privacy compliance, safeguarding information, privacy training, privacy laws, policies, and guidance, and contact information. Any questions, concerns, or complaints may be addressed by contacting the DOC Privacy Office by email at CPO@doc.gov or by telephone at (202) 482-1190.

2 Overview of the DOC Privacy Program

2.1 Mission Statement

The DOC is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information 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 consideration in all systems, programs, and policies.

2.2 Strategic Goals and Objectives for Privacy

The DOC Privacy Program supports all five core DOC missions as articulated in the DOC America is Open for Business 2014-2018 Strategic Plan, as well as the important cross-cutting goal to mature and strengthen economic growth by preserving privacy, oversight, and transparency in the execution of all Department activities. To accomplish the strategic outcomes, there are four DOC Privacy Program goals, each supported by specific and measurable objectives:

Department of Commerce Privacy Program Plan

GOAL 1

- **Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships**.

In promoting economic growth, DOC is entrusted to collect personal information from business, citizens, residents, and visitors. We are obligated to collect only the information that is necessary to carry out our missions and protect this data from misuse. Our core mission is to respect and protect individual privacy rights. We also have a duty to be accessible, transparent, and to provide as much information as possible to the public. The Department's privacy and disclosure professionals are integrated into the operations of each Bureau and Operating Unit. It is through this framework that the DOC Privacy Program is able to maintain one of its most valuable assets: the public trust.

- ✓ Objective 1.1 – Support DOC unity of effort by representing privacy and disclosure interests in departmental governance.
- ✓ Objective 1.2 – Provide guidance and issue policies related to privacy by leveraging the expertise of Privacy Officers and Privacy Points of Contact from across the Department using issue-based governance bodies.
- ✓ Objective 1.3 – Leverage the expertise of oversight and advisory bodies, advocates, and privacy experts from the private sector to foster dialogue and learn about emerging issues.

GOAL 2

- **Provide outreach, education, training, and reports in order to promote privacy and transparency.**

Privacy practices, principles, and protections are implicated in the Department's approach to implementing all of its missions. Privacy and the DOC missions are not traded or balanced, but rather are integrated in a manner that keeps the country safe and honors our core values. The DOC Privacy Program ensures that the Department's privacy protections and policies are understood by every DOC employee through education and training, and made known to the privacy community and public at large through extensive outreach.

- ✓ Objective 2.1 – Ensure consistent application of privacy and disclosure requirements, and Bureau and Operating Unit accountability across the Department.
- ✓ Objective 2.2 - Develop and deliver targeted and effective privacy training courses and materials to DOC personnel and other stakeholders through targeted educational and outreach opportunities tailored to DOC's broad constituency.
- ✓ Objective 2.3 - Cultivate and sustain a leadership role in the Federal privacy and disclosure communities.
- ✓ Objective 2.4 - Pursue proactive, timely disclosure of information about DOC programs, operations, systems, and policies in a manner that is easily accessible to Congress, the public, and oversight bodies.
- ✓ Objective 2.5 - Promote departmental privacy practices to international partners to advance the Fair Information Practice Principles (FIPPs) and build the confidence

necessary to fulfill the Department's mandate as it relies on international cooperation.

GOAL 3

- **Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DOC activities.**

Privacy protections are firmly embedded into the lifecycle of DOC programs and systems. In addressing new risks or adopting new and integrated approaches to protecting individual privacy, the privacy enterprise must identify early on any potential for infringement of core privacy values and protections, and address that risk accordingly. When issues are identified and resolved early, it helps ensure that programs and services provide the maximum public benefit with the least possible privacy risk.

- ✓ Objective 3.1 - Review, assess, and provide guidance to DOC programs, systems, projects, information sharing arrangements, and other initiatives to reduce the impact on privacy and ensure compliance.
- ✓ Objective 3.2 - Promote privacy best practices and guidance to the Department's information sharing and intelligence activities.
- ✓ Objective 3.3 - Ensure that complaints and incidents at DOC are reported systematically, processed efficiently, and mitigated appropriately in accordance with federal and DOC privacy policies and procedures.
- ✓ Objective 3.4 - Evaluate DOC programs and activities for compliance with privacy and disclosure laws.

GOAL 4

- **Develop and maintain the best privacy and disclosure professionals in the federal government.**

The human capital of the DOC is widely regarded as among the most talented privacy and disclosure professionals in the trade. This top tier talent is crucial to the Department's continued ability to implement its missions and to its success in maintaining the public trust. These professionals have continuously demonstrated agility in responding to new priorities and fiscal environments. Providing support, opportunities for professional growth and development, and a workplace environment in which they are valued are all crucial to recruiting and retaining a high performing workforce.

- ✓ Objective 4.1 - Reward exceptional employee performance and recognize individual contributions to advancing the office mission.
- ✓ Objective 4.2 - Support employee development and emphasize the role of training and professional development in performance planning.

2.3 DOC Privacy Office Organization

The Office of Privacy and Open Government (OPOG) within the Office of the Secretary (OS) provides oversight and management of the DOC Privacy Program. The Director of OPOG serves as the Department's SAOP and Chief Privacy Officer (CPO). The SAOP/CPO is the Department's key policy advisor on implementing the Privacy Act of 1974, 5 U.S.C. §552a, and

the privacy provisions of the Federal Information Security Modernization Act (FISMA) of 2014, and of the E-Government Act of 2002. The responsibilities of the SAOP/CPO include:

- Serving as the Department's senior policy authority on matters relating to the public disclosure of information, and advising on privacy issues related to informed consent, disclosure risks, and data sharing;
- Developing and overseeing implementation of Department-wide policies and procedures relating to the Privacy Act, and assures that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- Communicating the Department's privacy vision, principles and policies internally and externally;
- Ensuring the Department considers and addresses the privacy implications of all DOC regulations and policies, and leading the Department's evaluation of the privacy implications of legislative proposals, congressional testimony, and Office of Management and Budget (OMB) guidance;
- Advocating strategies for data and information collection and dissemination, to ensure Departmental privacy policies and principles are reflected in all operations;
- Ensuring Departmental policies and procedures regarding information protection are compliant with statutory and government-wide policy requirements, verifying bureau adherence to relevant information protection policies and procedures, and continually striving to identify and implement privacy best practices;
- Coordinating the Departmental process for reviewing and approving Privacy Impact Assessments (PIAs) to ensure compliance with the E-Government Act; managing the process for reviewing and approving privacy programs as part of the OMB budget process, and working with the Chief Information Officer to ensure that the FISMA authorization and accreditation process for new and existing systems appropriately addresses privacy-related issues;
- Managing privacy risks associated with DOC activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems;
- Ensuring the appropriate training and education regarding privacy laws, regulations, policies and procedures concerning the handling of personal information are afforded to employees and contractors; and
- Facilitating and negotiating agreements with senior management, and establishing relationships with partners in private industry and other federal agencies to foster the development and sharing of privacy-related best practices; and partners with the Office of the Chief Information Officer to ensure all aspects of the Privacy Program are incorporated into the Department's enterprise infrastructure, IT, and IT security program.

Additionally, the SAOP/CPO leads the office along with several deputies, support staff and contractors. The teams are managed by the Chief Privacy Compliance Officer, Deputy Director for Departmental Privacy Operations, and Deputy Director for the Freedom of Information Act (FOIA) and Privacy Act Operations. The Chief Privacy Compliance Officer serves as a key advisor on compliance with the Privacy Act, privacy requirements of the E-Government Act, including the FISMA, and the FOIA. The Deputy Director for Departmental Privacy Operations serves as the Department Privacy Program Coordinator for the review, coordination, and analysis

of personally identifiable information (PII) incidents and PIAs. The Deputy Director for FOIA and Privacy Act Operations provides operational oversight of the Department's FOIA and Privacy Act Program and processes to ensure bureau compliance with the FOIA/Privacy Act regulations.

2.4 Bureau Chief Privacy Officers

The DOC Privacy Program is implemented within its bureaus and operating units by the DOC Bureau Chief Privacy Officers (BCPOs). A Bureau Chief Privacy Officer is designated in each bureau/operating unit (B/OU) of the Department. The BCPOs assist the SAOP/CPO with implementing the DOC Privacy Program within the B/OUs. The BCPOs manage the individual B/OU portions of the DOC Privacy Program.

The DOC SAOP is ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within the B/OU. To ensure that B/OUs effectively carry out the privacy-related functions described in law and OMB policies, the DOC SAOP requires the head of each B/OU to designate a BCPO who has B/OU-wide responsibility and accountability for the B/OU's privacy program. The role and designation of the BCPO shall be governed by the following requirements:

- Position. The BCPO shall be a senior official (SES, GS-15 or equivalent level) who serves in a central leadership position at the B/OU, has visibility into relevant B/OU operations, and is positioned highly enough within the B/OU to regularly engage with other B/OU leadership, including the head of the B/OU.

- Expertise. The BCPO shall have the necessary skills, knowledge, and expertise to lead and direct the B/OU's privacy program and carry out the privacy-related functions described in law, and Office of Management and Budget (OMB) and DOC policies.

- Authority. The BCPO shall have the necessary authority at the B/OU to lead and direct the B/OU's privacy program and carry out the privacy-related functions described in law, and OMB and DOC policies.

2.5 DOC Privacy Council

The DOC Privacy Council, established by DOO 10-19, *Department of Commerce Privacy Council,* works to strengthen DOC privacy policies to ensure that they reflect the goals, values, and policies that the Department advocates. The Privacy Council is chaired by the SAOP/CPO and is comprised of the BCPOs. The Executive Council members include the Deputy Assistant Secretary for Administration, the Chief Information Officer, and the Assistant General Counsel for Administration from the Office of General Counsel.

The Privacy Council convenes monthly and routinely reviews Department privacy policies and identifies opportunities for strengthening, clarifying, and improving them, as well as identifies and recommends privacy training opportunities for DOC employees, as appropriate. A list of the authorities, memoranda, and policies is found in Appendix A.

2.6 DOC PII Breach Response Task Force

The DOC PII Breach Response Task Force is responsible for providing in-depth analysis and recommendations for an appropriate response to PII breaches that may cause significant harm to individuals or the Department. The DOC PII Breach Response Task Force is chaired by the SAOP/CPO. Members include the General Counsel, Chief Information Officer, Chief Financial Officer and Assistant Secretary for Administration, Assistant Secretary for Legislative and Intergovernmental Affairs, Chief of Staff in the Office of the Secretary, Director for the Office of Public Affairs, Director for the Office of Policy and Strategic Planning, Director for the Office of Human Resources Management, Office of Security (as needed), and Office of Inspector General in an advisory role.

The SAOP/CPO determines when to convene Task Force meetings for moderate risk, high risk, and major PII breach incidents. More information may be found in the DOC Privacy Act, Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan.

3 Privacy Workforce Management

The SAOP assesses and addresses the hiring, training, and professional development needs of the Department with respect to privacy, including providing input into the performance of employees who function in the capacity of a BCPO for any Departmental operating unit, as prescribed in DOO 20-31. Additionally, the SAOP coordinates with the Chief Information Officer and Chief Human Capital Officer to maintain and enhance a current workforce planning process, maintain workforce skills, recruit and retain privacy and IT professionals, develop a set of competency requirements for staff, and ensure managers are aware of flexible hiring authorities.

4 Budget and Acquisition

The SAOP reviews IT capital investment plans and budgetary requests to ensure that privacy requirements and associated privacy controls, as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. For IT acquisitions, the FY 2018 IT Compliance in Acquisition Checklist (Appendix B) is used to incorporate the applicable privacy clauses from the Federal Acquisition Regulation (FAR) to ensure the services, systems, and/or products being procured comply with existing privacy laws and policies regarding the protection, maintenance, dissemination, and disclosure of information. Additionally, the Privacy Requirements for Printing Services (Appendix C) ensures privacy requirements are included in the solicitation to select a vendor to provide a printing services solution.

5 Fair Information Practice Principles

The DOC Privacy Program adheres to the Fair Information Practice Principles (FIPPs). The Department uses these principles when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs include:

- Access and Amendment – Individuals are provided with appropriate access to PII and the opportunity to correct or amend PII.
- Accountability – The Department ensures compliance with these principles and applicable privacy requirements by monitoring, auditing, and documenting compliance. In addition, the roles and responsibilities with respect to PII for individuals are defined and appropriate training is provided to individuals who have access to PII.
- Authority – When B/OUs create, collect, use, process, store, maintain, disseminate, or disclose PII, the appropriate authorities are documented and placed in the appropriate notice.
- Minimization – B/OUs create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish the legally authorized purpose. The PII is maintained for as long as is necessary to accomplish the purpose.
- Quality and Integrity – B/OUs create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- Individual Participation – Individuals are involved in the process of using PII and, to the extent practicable, individual consent is granted for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to the DOC Privacy Office.
- Purpose Specification and Use Limitation – B/OUs provide notice of the specific purpose for which PII is collected and only use, process, store, maintain, disseminate, or disclose PII for the purpose that is explained in the notice.
- Security – Administrative, technical, and physical safeguards are established to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- Transparency – B/OUs provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

6 Privacy Risk Management Framework

The Department follows the process described in NIST SP 800-37 that incorporates information security and privacy risk management activities into the system development life cycle. This process includes:

- Categorizing each information system and the information processed, maintained, and transmitted by each system based on a mission or business impact analysis using NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
  1) The FIPS 199 security impact category is not the same as the NIST SP 800-122 PII

Confidentiality Impact Level. The categorization of PII is found in Appendix D.

- Selecting and implementing privacy and security controls and documenting how these controls are deployed for each information system;
- Assessing the privacy and security controls, including privacy continuous monitoring; and
- Obtaining SAOP approval prior to the 1) issuance of an Authorization to Operate (ATO) for a new system which will collect, process, share, and/or store personally identifiable information (PII); and 2) re-issuance/renewal of an ATO to authorize changes on a legacy PII processing, sharing, and/or storage system which will create new privacy risks, including adding a new collection of PII, as described in Commerce Policy Regarding 1) Implementing NIST 800-53 Revision 4, Appendix J Privacy Controls and 2) SAOP Approval as a Precondition for the Issuance of an Authorization to Operate (ATO).

7 Privacy Control Requirements/Continuous Monitoring Strategy

The DOC ensures compliance with all applicable statutory, regulatory, and policy requirements. The DOC implements the NIST SP 800-53, Rev 4 baseline of security and privacy controls, including Privacy Overlays. The DOC adheres to Section 208 of the E-Government Act of 2002, which requires agencies to conduct Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs) for electronic information systems and collections. In addition, the DOC meets Privacy Act System of Records Notice (SORN) requirements.

7.1 DOC Appendix J Control Allocation Table

The DOC SAOP designates which privacy controls the Department will treat as program management, common, information system-specific, and hybrid controls. Privacy program management controls are controls that are generally implemented at the agency level and essential for managing the agency's privacy program. Common controls are controls that are inherited by multiple information systems. Information system-specific controls are controls that are implemented for a particular information system or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system in part as a common control and in part as an information system-specific control. The determination as to whether a privacy control is a common, hybrid, or information system-specific control is based on context. The Appendix J Control Allocation Table is found in Appendix E.

7.2 DOC Privacy Overlays

The DOC Privacy Program leverages privacy overlays established for national security systems as guidance when selecting/assessing effectiveness of privacy protections. According to NIST SP 800-53, Revision 4, an overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The purposes of

the privacy overlays include providing standard security and privacy control baselines for systems containing PII, ensuring integration of privacy considerations into the system development life cycle and security processes in the early stages, and providing guidance for privacy requirements for protected health information. Summarized information on implementing privacy overlays is found in Appendix F. The entire DOC Privacy Overlays document can be found on the DOC Privacy website at www.commerce.gov/privacy.

7.3 Privacy Threshold Analysis (PTA)

A privacy threshold analysis (PTA) is a questionnaire used to determine if a system contains personally identifiable information (PII), whether a PIA is required, whether a SORN is required, and if any other privacy requirements apply to the information system. A PTA is completed when proposing a new information technology system through the budget process that collects, stores, or processes identifiable information; when developing or significantly modifying such a system; or when proposing a new electronic collection of identifiable information. A PTA determines if a PIA is required. The PTA Template is found in Appendix G.

The Department also has a PTA for information collections and forms. The Forms PTA (Appendix H) must accompany all information collections submitted as a part of the Paperwork Reduction Act process.

7.4 Privacy Impact Assessment (PIA)

A PIA is an analysis of how information in identifiable form is collected, maintain, stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks. A PIA is conducted before:

A. Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form, from or about, members of the public; or
B. Initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

If a PIA is required, the Information System Security Officer (ISSO) and System Owner (SO) work closely with the Information Technology Security Officer (ITSO) to complete the PIA Template (Appendix I). Once completed, it is reviewed by the BCPO. When the BCPO certifies the PIA, both the PTA and PIA are forwarded to the Department's OCIO and SAOP/CPO for review. A PIA Compliance Review Board (CRB) meeting is held, if deemed necessary by the Chief Privacy Compliance Officer. Once the SAOP/CPO approves the PIA, the PTA and PIA are made publicly available on the Department's privacy website at www.commerce.gov/privacy, unless the Department determines not to make the PIA publicly available if such publication would raise security concerns, reveal issues of national security, classified information, or reveal sensitive information that could be potentially damaging to a national interest, law enforcement effort, or competitive business interest. A flowchart of the PIA process is found in Appendix J.

7.5 PIA Compliance Review Board (CRB) Meetings

The SAOP conducts PIA CRB meetings with the BCPOs, ISSOs, ITSOs, SOs, and/or Authorizing Officials (AOs) to discuss system/data characterization, information sharing practices, website/mobile application processes, privacy controls, and risk assessments for new

systems processing PII and existing systems with changes that create new privacy risks. The PIA CRB Risk Analysis Guide (Appendix K) outlines the critical areas discussed during these meetings

Through the continuous monitoring program, PTAs are completed annually to determine if a PII processing system has changes that create new privacy risks. If so, the PIA is updated and a CRB is held to ensure compliance with applicable laws and regulations. Otherwise, the latest SAOP approved PIA is submitted to the SAOP/CPO with the Privacy Impact Assessment Annual Review Certification Form (Appendix L). A CRB must be conducted every three (3) years.

Amended PIAs are immediately required when a Major Change occurs which creates new privacy risk, as defined by OMB Memorandum 03-22.

7.6 Contractors and Third Parties

The DOC ensures contractors and third parties that: 1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of the Department; or 2) operate or use information systems on behalf of the Department, comply with the mandated privacy requirements. The DOC Privacy Program coordinates with the Office of Acquisition Management to ensure that the applicable privacy clauses, below from the FAR, are included in the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of information in the possession of the Department:

- FAR Subpart 4.19 – Basic Safeguarding of Covered Contractor Information Systems
  - FAR Clause 52.204-21
- FAR Subpart 24.1 Protection of Individual Privacy
  - FAR Clause 52.224-1 “Privacy Act Notification”
  - FAR Clause 52.224-2 “Privacy Act”
- FAR 39.101 – Acquisition of Information Technology-General-Policy
- FAR 39.105 – Acquisition of Information Technology-General-Privacy
  - FAR Clause 52.239-1 “Privacy or Security Safeguards”
- FAR Subpart 27.4 – Rights in Data and Copyrights

These FAR clauses are also included in the IT Compliance in Acquisition Checklist found in Appendix B.

7.7 System of Records Notice (SORN)

The DOC meets Privacy Act requirements for publishing publish notices of its systems of records in the Federal Register which are referred to as SORNs. A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

A SORN is intended to inform the public about what kinds of personal information federal agencies maintain; to limit the uses and disclosures of the information to those compatible with the law permitting its collection; and to describe how an individual might request access to their

information or to seek redress otherwise.

- Bureau and Operating Unit (Component) Notices – Component systems of records are records for which a DOC component such as the Census Bureau, writes the SORN for the records for which they have physical custody and maintain. The following characteristics also apply:
  - The physical records contained within the system of records belong to the respective component; and
  - The corresponding SORNs begin with the component's identifier (e.g., CENSUS-1, 2, etc.).
- Department-wide Notices – Systems of records for which the Department writes the SORN for the records, but may not have physical custody as a matter of necessity. The Department's components may use Department-wide SORNs to cover records systems they maintain. The following characteristics apply to Department-wide notices:
  - The physical records contained within the system of records belong to the respective component;
  - The Department may still retain some authority over the records; and
  - The corresponding SORNs begin with the identifier DEPT-1, 2, etc.
- Government-wide Notices – Systems of records for which another Federal agency, such as the Office of Personnel Management (OPM), writes the SORN for the records, but does not have physical custody as a matter of necessity, as in the case of general personnel records. Federal agencies may use Government-wide SORNs to cover Government-wide records systems and the following characteristics apply:
  - The physical records contained within the system of records belong to the respective agency;
  - OPM, for example, still retains some authority over the records; and
  - The corresponding SORNs begin with the identifier GOVT-1, 2, etc.

7.7.1 SORN Reviews and Updates

The DOC ensures that SORNs remain accurate, up-to-date, and appropriately scoped during B/OU PIA reviews and as part of the DOC PIA CRB process. The DOC also uses a CRB meeting to ensure that with respect to SORNs:

- No system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order; and
- Each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary.

BCPOs are responsible for obtaining B/OU Unit Privacy Act Officer concurrence with the SORN(s) cited to cover system(s) of records identified in a PIA. When a SORN needs to be amended or created to cover a system of records, the B/OU Privacy Act Officer works with the appropriate B/OU subject matter experts and the Departmental Privacy Act Officer (DPAO) to draft the amended or new SORN(s), ensuring that the SORNs include the information required by and are in the format identified in OMB Circular A-108. The template for a new/modified SORN is found in Appendix M. The template for the rescindment of a SORN is found in

Appendix N.

7.7.2 Reporting SORNs to OMB and Congress

The SAOP and the DPAO report all significant changes to SORNs and new SORNs to OMB and Congress following requirements identified in OMB Circular A-108. Reports include a transmittal letter signed by the SAOP and a narrative statement, generally prepared by the appropriate B/OU Privacy Act Officer, that contain the following elements:

- A description of the purpose(s) for which the DOC is establishing or modifying the system of records and an explanation of how the scope of the system is commensurate with the purpose(s) of the system;
- The specific authorities (statutes or executive orders) under which the system of records will be maintained. The DOC cites the specific programmatic authorities for collecting, maintaining, using, and disseminating the information;
- An evaluation of the probable or potential effect of the proposal on the privacy of individuals whose information will be maintained in the system of records; the assessment may be derived from applicable PIAs;
- An explanation of how each new or modified routine use satisfies the compatibility requirement of the Privacy Act; and
- Any information collections approved by OMB or submitted to OMB for approval that will be used to collect information that will be maintained in the system of records, along with the relevant names, OMB control numbers, and expiration dates.

7.8 Privacy Act Statement

The DOC ensures that a Privacy Act compliant statement is provided or available when collecting PII. The Privacy Act Statement is provided on the collection instrument, on a poster that is visible to the individual, or on a separate form that can be retained by the individual prior to the actual collection. A Privacy Act Statement provides an individual with the:

- Agency's legal authority to collect the information, such as a statute, executive order, and/or regulation;
- Purpose(s) for collecting the information and how it will be used;
- Routine uses of the information, which describes to whom the Department may disclose information outside of the Department and for what purposes[1]; and
- Whether providing the information is mandatory or voluntary, along with the effects, if any, on the individual of not providing all or any part of the information requested.

8 Overview of Requirements for Handling and Protecting Personally Identifiable Information (PII)/Business Identifiable

[1] The DOC also includes appropriate citation to the relevant SORN(s), including link(s) if practicable.

Information (BII)

Handling and safeguarding PII in the Department's possession is fundamental to ensure the public's trust. At the Department, BII must be similarly protected as PII, in accordance with applicable laws. In an effort to protect all data, the Departmental Privacy Standards for Commerce Data Loss Prevention (DLP) Security Tools establishes a requirement for B/OUs to configure their DLP security tools to implement privacy control capabilities that enhance privacy protections and reduce PII breaches within the Department.

8.1 Recognizing Personally Identifiable Information (PII)

Personally Identifiable Information (PII) refers to information which can be used to distinguish or trace an individual's identity. PII includes, name, social security number, biometric records, etc. which alone, or combined with other personal or identifying information, such as date and place of birth, mother's maiden name, etc. can be linked to a specific individual.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. The following types of PII are considered sensitive when associated with an individual:

- Social Security Number (including in 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/purchase card account numbers;
- Passport numbers;
- Potentially sensitive employment information (e.g., performance ratings, disciplinary actions, results of background investigations);
- Criminal history; or
- Information that may stigmatize or adversely affect an individual.

Context of information is 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's softball roster is very different from a list of names and phone numbers for individuals being treated for an infectious disease.

8.2 Recognizing Business Identifiable Information (BII)

Business Identifiable Information is 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." This information is exempt from automatic release under the FOIA exemption. "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 can include information submitted by a nonprofit entity; or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g.,

13 U.S.C. 9).

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. 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, and financial records collected as part of an investigation.

8.3 Minimizing the Collection of PII/BII

The Privacy Act of 1974 requires that Federal agencies maintain only relevant and necessary information about individuals. In addition, the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, directs Federal agencies to eliminate unnecessary collections, maintenance, and uses of Social Security Numbers (SSN).

The DOC maintains a Department-wide inventory of PII/BII holdings and uses the PTA, PIA, and SORN certification and re-certification process to identify reduction opportunities and to ensure, to the maximum extent practicable, that such holding is accurate, relevant, timely, and complete. In addition, the Department has established process requirements for justifying the collection, maintenance, and uses of SSNs as directed in DOC Social Security Numbers (SSNs) Justification Process Memorandum (June 20, 2017).

8.4 Handling and Transmitting PII/BII

PII requires strict handling guidelines due to the nature of the data and the increased risk to an individual if data were to be compromised. Ways of handling PII/BII include:

- Encrypt sensitive PII/BII on computers, media, and other devices;
- Lock or log off unattended computer systems;
- Destroy sensitive paper PII/BII by shredding or using burn bags;
- Delete sensitive electronic PII/BII by emptying computer “recycle bin”;
- Store sensitive PII/BII on secure Federal Government systems only;
- Secure sensitive paper PII/BII data by locking in desks and filing cabinets.

Sensitive PII/BII may be distributed or released to other individuals if it is within the scope of their official duties and they have a need to know. If sensitive PII/BII is electronically transmitted, it must be protected by secure methodologies, such as encryption, Public Key Infrastructure, or secure sockets layer. When in doubt, treat PII as sensitive. The transmission of sensitive PII and BII must be kept to a minimum, even if it is protected by secure means.

Other ways for communicating, sending, and receiving sensitive PII/BII include:

- Facsimile – When faxing information, include an advisory statement about the contents on the cover sheet and notify the recipient before and after transmission. Exception: According to Commerce Acquisition Manual 1313.301, DOC purchase card holders shall not transmit purchase card information over a facsimile machine.

- Mail – Physically secure sensitive PII/BII when in transit by sealing it in an opaque envelope or container, and mail using First Class or Priority Mail, or a commercial delivery service. Do not mail, or send by courier sensitive PII/BII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.
- Hard Copy – Hand-deliver documents containing sensitive PII/BII if needed. Do not leave sensitive PII/BII unattended on printers, facsimile machines, or copiers.

8.5 Understanding Commerce Website Privacy Policy

The Commerce website privacy policy establishes how information obtained from individuals when visiting the Commerce website will be handled. The privacy of our visitors is of utmost importance. No PII is collected when visiting the website unless the individual chooses to provide the information.

9 Breach Incident Response and Management

The Department has a duty to appropriately safeguard all PII in its possession and to prevent compromise of this information in order to maintain the public's trust. The Privacy Act, PII, and BII Breach Notification Plan serves to inform all employees, contractors, bureaus, and operating units of the DOC of their obligation to protect PII and establish procedures to define how to prepare for and respond to any breach incidents.

Additionally, the *Procedures on Notifying Management Officials of Individuals Who Fail to Safeguard Sensitive PII* can be used by the BCPOs to ensure managers, supervisors, and/or contracting officer representatives are made aware of a PII breach in a timely manner.

OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, provides the policy for Federal agencies to prepare for and respond to a breach of PII. The DOC Privacy Office works closely with the BCPOs and the Enterprise Security Operations Center (ESOC) within the OCIO to ensure a PII breach is expeditiously reported, handled, and closed appropriately.

BCPOs must ensure:

- All sensitive PII breach incidents are reported to the ESOC and the SAOP/CPO within one (1) hour of discovery/detection.
- All sensitive PII breach incidents are under investigation within 48 hours of the incident discovery/detection.
- A follow-up report is completed and submitted to the ESOC and the SAOP/CPO.
- All corrective/remedial actions for each PII incident are confirmed completed prior to the close-out of a low risk PII incident. SAOP/CPO concurrence must be granted prior to the close-out of a moderate risk, high risk, and/or Major PII incident.

BCPOs must complete and submit a Summary Incident Report (Appendix O) to the SAOP/CPO at CPO@doc.gov within the following timeline:

- Major PII Incident – within 24 hours
- High Risk PII Incident – within three (3) work days
- Moderate Risk PII Incident – within three (3) to five (5) work days

The ESOC provides notification of all cyber related (electronic) PII incidents with confirmed loss of confidentiality, integrity, or availability to the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT) within one (1) hour of being reported. If an assessment has been made that a PII breach constitutes a Major incident, the ESOC reports the designation to US-CERT as soon as the Department has a reasonable basis to conclude that such a PII breach has occurred. The ESOC reports all non-cyber related (paper) incidents to the SAOP/CPO within one (1) hour of a confirmed breach.

10 Awareness and Training

As Commerce strives to be a leader in best privacy practices and privacy policy, the Department requires a mandatory privacy performance element in every employee performance plan. This ensures high priority is assigned to privacy considerations in all systems, programs, and policies. The Commerce Privacy Training Program promotes maximum employee and contractor understanding and adherences to Fair Information Practice Principles (FIPPS). Based on the need, different levels of training are offered or are mandatory for employees and contractors.

The Department conducts activities promoting privacy and security awareness, such as Privacy Day, Sunshine Week, Cybersecurity Awareness Day, and Security Awareness Day. During these events, the following privacy brochures are discussed and distributed to employees, contractors, and visitors:

- How to Protect PII and BII when Transmitting to Authorized Users
- PII Breach Incident Reporting
- Privacy Impact Assessments
- DOC's Quick-Start Guidance for Moving Sensitive PII/BII

10.1 New Employee Orientation Training

New employee orientation sessions across the Department include presentations on how to handle privacy protected information, and Privacy Act information protection requirements. Privacy brochures which provide definitions and examples of PII and BII, along with step by step procedures on how to use the Department's suite of encryption and secure file transfer technologies to protect sensitive PII transmitted electronically are distributed to all new employees during orientation.

10.2 Commerce Learning Center Training

The Commerce Learning Center (CLC) delivers privacy specific courses to Commerce employees and contractors as part of the suite of mandatory annual IT Security/Privacy training. Contractors who do not have access to CLC are provided the same training in a presentation format.

In addition, dedicated role-based privacy training is provided to offices and individuals who regularly handle specific categories of privacy protected information.

10.3 Bureau/Operating Unit (B/OU) Training

The B/OUs conduct bureau specific privacy training for employees and contractors. Some of the training sessions are separated for supervisory and non-supervisory employees.

11 Privacy Reporting

11.1 Annual Report- Federal Information Security Modernization Act (FISMA)

The Federal Information Security Modernization Act (FISMA) of 2014 requires Federal agencies to develop, document, and implement agency-wide information security programs that include plans and procedures to ensure the continuity of operations for information systems that support the operations of the agencies. All Federal agencies are required to submit an annual report to the OMB and U.S. Department of Homeland Security; the Committees on Oversight and Government Reform, Homeland Security, and Science, Space, and Technology of the House of Representatives; the Committees on Homeland Security and Government Affairs; and Commerce, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; and the Comptroller General.

11.2 Quarterly Report - Chief Financial Officer & Assistant Secretary for Administration (CFO/ASA) Privacy Metrics

The operating units with the CFO/ASA must submit and present quarterly metrics on specific programs to the Department Management Council and Chief Executive Officers. The PII incident metrics are a part of the quarterly reporting.

11.3 Enterprise Security Operations Center (ESOC) Quarterly Reporting

At the end of each quarter of the fiscal year, the Enterprise Security Operations Center (ESOC) provides a report to the DOC SAOP detailing the status of each breach reported to the ESOC during the fiscal year. The DOC SAOP reviews the report and validates that the report accurately reflects the status of each reported breach.

12 Conclusion

The DOC is committed to safeguarding PII/BII. The DOC Privacy Program intends to use all methods of regulation, policy, guidance, and principles to further this objective across the Department of Commerce. Privacy considerations are a part of all levels of decision-making in an effort to continuously build a culture of trust and privacy throughout each B/OU.

13 Appendices

Appendix A – Authorities, Memoranda, Policies, and Guidance
Appendix B – IT Compliance in Acquisition Checklist
Appendix C – Privacy Requirements for Printing Services
Appendix D – Categorizing Personally Identifiable Information (PII)
Appendix E – Appendix J Control Allocation Table

Appendix A – Authorities, Memoranda, Policies, and Guidance

Authorities

- Privacy Act of 1974, 5 U.S.C. §552a
- Federal Information Security Modernization Act of 2014
- E-Government Act of 2002
- Freedom of Information Act (FOIA)
- Trade Secrets Act
- Paperwork Reduction Act of 1995
- Children's Online Privacy Protection Act of 1998

Office of Management and Budget (OMB) Memoranda

- OMB Memorandum for Privacy Act Officers of Departments and Agencies, *Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act (June 21, 2000)*
- OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy (December 20, 2000)*
- OMB Memorandum M-03-22**,** *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)*
- OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010)*
- OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Application, (June 25, 2010)*
- OMB Memorandum for Chief Information Officers, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications, (December 29, 2011)*
- OMB Memorandum M-13-13, *Open Data Policy-Managing Information as an Asset (May 9, 2013)*
- OMB Memorandum M-13-20, *Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative (August 16, 2013)*
- OMB Memorandum M 14-06, *Guidance for Providing and Using Administrative Data for Statistical Purposes, (February 14, 2014)*
- OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)*
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services (November 8, 2016)*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets, (December 9, 2016)*
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)*

OMB Circulars

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016)*
- OMB Circular A-130, *Managing Information as a Strategic Resource (July 28, 2016)*
- OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 23, 2016)*

Department of Commerce (DOC) Policies

- Commerce Policy Regarding 1) Implementing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Appendix J Privacy Controls, and 2) Senior Agency Official for Privacy (SAOP) Approval as a Precondition for the Issuance of an Authorization to Operate (ATO) (November 18, 2014)
- Procedures on Notifying Management Officials of Individuals Who Fail to Safeguard Sensitive Personally Identifiable Information (PII) (August 3, 2015)
- Departmental Privacy Standards for Commerce Data Loss Prevention (DLP) Security Tools (April 15, 2016)
- DOC Social Security Numbers (SSNs) Justification Process Memorandum (June 20, 2017)

Bureau/Operating Unit Privacy Policies

- Commerce Privacy Policy
- Bureau of Economic Analysis (BEA) Privacy Policy
- Bureau of Industry and Security (BIS) Privacy Policy
- Bureau of the Census Privacy Policy
- Economic Development Administration (EDA) Privacy Policy
- Economics and Statistics Administration (ESA) Privacy Policy
- International Trade Administration (ITA) Privacy Policy
- Minority Business Development Agency (MBDA) Privacy Policy
- National Oceanic and Atmospheric Administration (NOAA) Privacy Policy
- National Institute of Standards and Technology (NIST) Privacy Policy
- National Telecommunications and Information Administration (NTIA) Privacy Policy
- National Technical Information Services (NTIS) Privacy Policy
- Office of Inspector General (OIG) Privacy Policy
- Office of the Secretary (OS) Privacy Policy
- United States Patent and Trademark Office (PTO) Privacy Policy

DOC Privacy Guides and Brochures

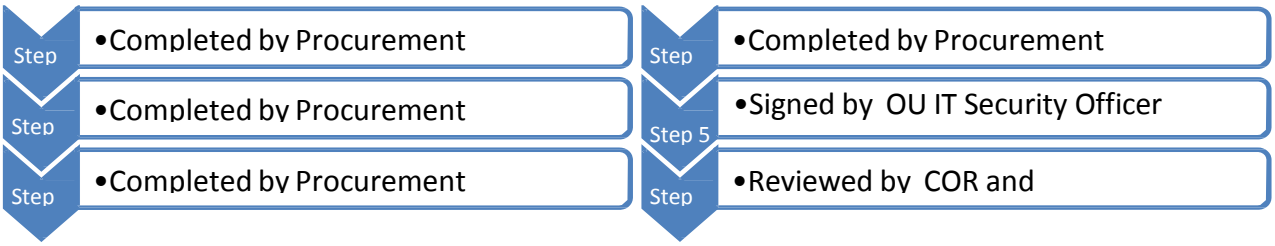
- Quick-Start Guidance for Moving Sensitive Personally Identifiable Information (PII) and Business Identifiable Information (BII)
- How to PROTECT Personally Identifiable Information (PII) and Business Identifiable Information (BII) When Transmitting to AUTHORIZED USERS using Accellion.
- Personally Identifiable Information (PII) Breach Incident Reporting
- Privacy Impact Assessments (PIA) Brochure

Appendix B – IT Compliance in Acquisition Checklist

Instructions:

This IT checklist, with appropriate signatures, must be completed for Information Technology (IT) acquisitions within the Department of Commerce (DOC). It represents a list of important or relevant actions (steps) that must be taken to ensure that security considerations are incorporated into IT acquisitions. *Note: Completion of this checklist is not required for the acquisition of equipment for specialized Research and Development (R&D) or scientific purposes that are not a National Security System.*

In completing the checklist, you can assume that if the answer to a question does not redirect you to a new question further down the checklist, you should proceed to the next question until you obtain the final concurrence signatures. Each checklist question should be addressed in coordination with the Acquisition team including: The Procurement Requestor from the program office, the Procurement Contracting Officer Representative (COR), Operating Unit Approved Program/ Requesting Office IT Security Officer, and Acquisition Contracting Official (CO).



Background:

This checklist was developed to ensure that the acquisition of IT resources complies with Federal and DOC information security policy requirements and to provide a means for COs to document compliance.

	System(s): *[Provide full name of system(s) and any corresponding acronym(s)]* **Procurement Description:** *[Provide 1-2 sentences on what the IT acquisition is for]*	**Date:**
1	**Does this acquisition involve a hardware or software product purchase?** If the answer is No, proceed to question 2. If the answer is Yes, include appropriate clauses into the solicitation and contract to ensure this acquisition meets the following: • DOC IT Security Program Policy ITSPP media sanitization requirements (MP-6) • FAR 39.101(d) regulations involving NIST common security configuration checklists including Federal Desktop Core Configuration (FDCC) or United States Government Configuration Baseline (USGCB) initiative • Personal identity verification requirements from FAR 4.1302 and FIPS PUB 201 [in accordance with Homeland Security Presidential Directive (HSPD-12)] • FAR part 11.002 requirements which state that *unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication (SP) 500-267)* and the corresponding declarations of conformance defined in the USGv6 Test Program. *To meet this requirement each DOC acquisition of IP protocol technology must express requirements for IPv6 capabilities in terms of the USGv6 Profile (i.e., using the USGV6 Capabilities Check List) and vendors must be required to document their product's support of the requested capabilities through the USGv6 test program (reference http://www.antd.nist.gov/usgv6/) using the USGv6 Suppliers Declaration of Conformity.* Proceed to question 2.	Yes ☐ No ☐

2	**Will any personnel involved in this acquisition perform a function/role that requires access to a system(s) that processes non-public or sensitive DOC data?** *For example, requiring a DOC e-mail account, system administrator access to a DOC system, vendor installation/maintenance, contractor personnel operating system(s) that process DOC data, or DOC entrusted personally identifiable information (PII) being transferred to, shared with, and/or accessed by a contractor.* If the answer is No, proceed to question 3. If the answer is Yes, Contracting Officials should work with the COR to incorporate contract language from Commerce Acquisition Regulation (CAR) Final Rule 48 CFR 13, specifically: • Determine and document contract risk using the Commerce Acquisition Manual 1337.70. Insert the appropriate clauses into the contract based on risk level. Select from the following Security Processing Requirements: *1)* High or Moderate Risk Contracts -- 48 CFR Ch. 13 1352.237-70 *2)* Low Risk Contracts – 48 CFR Ch. 13 1352.237.71 *3)* National Security Contracts – 48 CFR Ch. 13 1352.237.72 *4)* Foreign National Visitor and Guest Access to Departmental Resources • Determine and document appropriate FISMA requirements to be met in the contract, and assist in the coordination with DOC Office of Security (OSY) for personnel screenings, see Chapter 11 Investigative Processing, of the Manual of Security Policies and Procedures, and the IT Security Office involving DOC ITSPP requirements for a Security Assessment & Authorization (A&A). • Take appropriate action, in consultation with the COR, OSY, and DOC Office of General Counsel, regarding the personnel screening forms. • Determine the appropriateness of allowing interim access to DOC IT systems pending favorable completion of a pre-employment check. • Incorporate appropriate clauses from FAR *1352.239-72 Security Requirements for Information Technology Resources* into the solicitation and contract to ensure that the requirements, such as annual IT security awareness training, are enforceable on contract personnel. • Take appropriate action and incorporate the applicable privacy clauses below from the FAR, in consultation with your Privacy Officer, to ensure that the services, systems, and/or products being procured comply with existing privacy laws and policies regarding protection, maintenance, dissemination and disclosure of information. • FAR Subpart 4.19— Basic Safeguarding of Covered Contractor Information Systems • FAR Clause 52.204–21 • FAR Subpart 24.1—Protection of Individual Privacy • FAR Clause 52.224-1 “Privacy Act Notification” • FAR Clause 52.224-2 “Privacy Act” • FAR 39.101—Acquisition of Information Technology—General—Policy • FAR 39.105—Acquisition of Information Technology—General–Privacy • FAR Clause 52.239-1 “Privacy or Security Safeguards” • FAR Subpart 27.4--Rights in Data and Copyrights • In consultation with the Contracting Officer, make sure FAR and all other applicable clauses protecting personal privacy interests are included (e.g., 48 CFR 24.104). Proceed to question 3.	Yes ☐ No ☐

3	**Will this acquisition involve Government property located at an off-site contractor-controlled facility that will be used for transmitting, processing, and storing DOC data?**
	
	If the answer is No, proceed to question 4.
	If the answer is Yes, include FAR *1352.239-72, Security Requirements for Information Technology Resources,* and incorporate the applicable privacy clauses below from the FAR, into the solicitation and contract. Initiate the appropriate Security Assessment & Authorization (A&A) of the contractor system(s) involved and include clauses to ensure this acquisition meets DOC ITSPP security requirements for transmitting, processing, and storing data.
	• FAR Subpart 4.19— Basic Safeguarding of Covered Contractor Information Systems
	  • FAR Clause 52.204–21
	• FAR Subpart 24.1—Protection of Individual Privacy
	  • FAR Clause 52.224-1 "Privacy Act Notification"
	  • FAR Clause 52.224-2 "Privacy Act"
	• FAR 39.101—Acquisition of Information Technology—General—Policy
	• FAR 39.105—Acquisition of Information Technology—General–Privacy
	  • FAR Clause 52.239-1 "Privacy or Security Safeguards"
	• FAR Subpart 27.4--Rights in Data and Copyrights
		Yes ☐ No ☐

4	**Will this acquisition involve a service level agreement?** *For example, contractor maintenance on DOC system hardware or software, Software as a Service (SaaS), i.e., Cloud Computing, or External Data Storage or Contingency Emergency Back-up facility.* If the answer is No, proceed to question 5. If the answer is Yes, initiate appropriate Security Assessment and Authorization of the contractor system(s) involved and include clauses to ensure this acquisition meets DOC ITSPP security and privacy requirements for transmitting, processing, and storing data, NIST SP 800-37 Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (sp800-37-rev1-final.pdf) and SP 800-64 Revision 2, *Security Considerations in the Information System Development Life Cycle* (SP800-64-Revision2.pdf) involving nondisclosure of information. Ensure that data portability, data breach notification, and data disposal are considered in the contract. Insert clauses from Commerce Acquisition Manual 1337.70 Section 3.3 IT Service Contracts, into the contract. Also, ensure FAR part 11.002 requirements cited on page 1, question 1 of this checklist are followed. Proceed to question 5.	Yes ☐ No ☐

5	**Supply Chain Risk Assessment Requirements** **Part 1 – Section 515 Supply Chain Risk Assessment (SCRA) Applicability:** **5A. Is this an acquisition of new high-impact or moderate-impact information system?** (A new high-impact or moderate-impact information system is defined as: acquisition of a new information system that is designated as FIPS 199 moderate-impact or high-impact; is subject to the reporting requirements of 44 U. S. C. Section 3505(c) FISMA Reportable System; and for which a new system inventory record will be created and entered into the CSAM in accordance with CITR- 019 Risk Management Framework (RMF). Reference CITR – 023: Pre-Acquisition Supply Chain Risk Assessment Section 6.1 at https://connection.commerce.gov/policy/20140528/it-security-program-policy-commerce-information-technology-requirements-and-policy.) If the answer to 5A is Yes, a SCRA is required. If the answer to 5A is No, a SCRA is not required. **Part 2 – National Security System (NSS) SCRA Applicability:** **5B. Is this an acquisition for a NSS (Classified or Unclassified), including IT equipment and software?** **5C If the answer to 5B is Yes, is the acquisition exclusively for any of the following types of items?** - Cabling (i.e. Cat 5 or Fiber Optic) - Cable Adaptors - Power Cable - Network Server Rack - Keyboard (Wired) - Mouse (Wired) - Items with no integrated circuitry (i.e. Monitor stands) If the answer to 5C is Yes, a SCRA is not required. If the answer to 5C is No, a SCRA is required. *The OU OCIO or designee has reviewed this purchase and confirmed a SCRA is or is not applicable.* **Name:** **Phone:** **Signature:** **Date:** **If a SCRA is required, a warranted CO shall conduct the buy, add required language in solicitation and contract documents, and transmit vendor-provided information to the OU OCIO or designee.**	Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐

6	**Do you have any supplemental information to add to this checklist?** If the answer is No, proceed to *Signatures* section below to obtain signatures. If the answer is Yes, please attach appropriate supplemental information (i.e., project org chart, previous acquisition checklist) to this checklist and proceed to *Signatures* section below to obtain signatures.	Yes ☐ No ☐

Signatures:

By signing this checklist, the Information System Security Officer, Procurement COR, IT Security Officer and Contracting Officer are representing that operating unit information security management oversight and appropriate due diligence were considered for this acquisition process.

Cognizant Office of Chief Information Officer Representative (OCIO) (if needed):

Name:	**Phone:**
Signature:	
Date:	

Information System Security Officer (ISSO):

Name:	**Phone:**
Signature:	
Date:	

Bureau Chief Privacy Officer (BCPO):

Name:	**Phone:**
Signature:	
Date:	

Procurement COR:

Name:	**Phone:**
Signature:	
Date:	

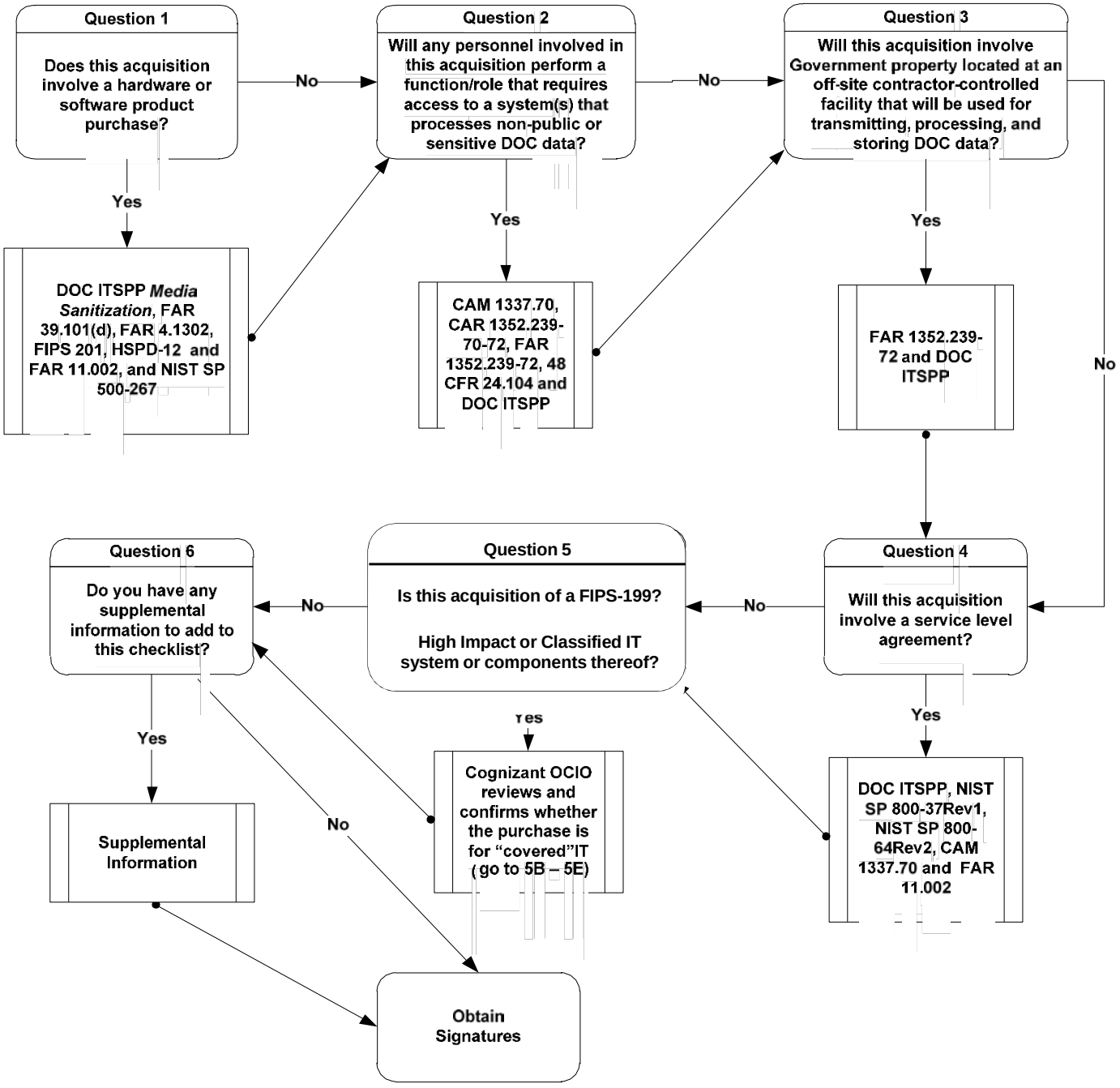
Operating Unit approved Program/Requesting Office IT Security Officer:

Name:	**Phone:**
Signature:	
Date:	

Contracting Officer:

Name:	**Phone:**
Signature:	
Date:	

IT Security Compliance in Acquisition Checklist



References:

Definition of Information Technology: includes hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. [return to instructions]

Commerce Acquisition Manual Chapter 1337.70: Personnel Security Processing Requirements for DOC Service
http://www.osec.doc.gov/oam/acquistion_management/policy/commerce_acquisition_manual_cam/documents/CAM_1337-700_Personnel_Security_Requirements.pdf

Commerce Office of Security (OSY) Manual of Security Policies and Procedures:

http://home.osec.doc.gov/osy/SecurityManual/Security%20Manual.pdf

Federal Acquisition Regulation (FAR) Case 2005-041, Internet Protocol Version 6 (IPv6):

http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf

Federal Acquisition Regulation (FAR) Subpart 4.13: Personal Identity Verification
https://www.acquisition.gov/far/current/html/Subpart%204_13.html

Federal Acquisition Regulation Part 11.0002 (G) Policy: Acquiring information technology using Internet Protocol https://www.acquisition.gov/far/html/Subpart%2011_1.html#wp1086792

Federal Desktop Core Configuration (FDCC): OMB M-07-18, Ensuring New Acquisitions Include Common Security Configurations,
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-18.pdf

IT Security Program Policy:
(http://home.commerce.gov/CIO/ITSITnew/DOC%20_TSPP_2009_Final_.pdf)

National Checklist Program (NCP): United States Government Repository of Publicly Available Security Checklists (http://web.nvd.nist.gov/view/ncp/repository)

NIST FIPS PUB 201-1 Change Notice 1: Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

NIST SP 500-267: A Profile for IPv6 in the U.S. Government – Version 1.0,
July 2008, http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

NIST SP 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010, (sp800-37-rev1-final.pdf)

NIST SP 800-64 Revision 2: Security Considerations in the Information System Development Life Cycle, Revision 2, October 2008, (SP800-64-Revision2.pdf)

NIST SP 800-70 Revision 2: National Checklist Program for IT Products - Guidelines for Checklist Users and Developers, February 2011, http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf

Security Content Automation Protocol (SCAP) Validated Products: http://nvd.nist.gov/scapproducts.cfm

United States Government Configuration Baseline (USGCB): USGCB baseline initiative evolved from the Federal Desktop Core Configuration mandate (http://usgcb.nist.gov/index.html)

USGv6: A Technical Infrastructure to Assist IPv6 Adoption: http://www.antd.nist.gov/usgv6/

We appreciate your continued efforts to make the Department's IT security posture more effective and efficient. If you have any questions, please contact the Office of Cyber Security at DOCITSecurity@doc.gov.

Appendix C – Privacy Requirements for Printing Services

U.S. DEPARTMENT OF COMMERCE
PRIVACY REQUIREMENTS FOR PRINTING SERVICES

SECTION 1. PURPOSE.

To ensure privacy requirements are included in a solication to select a vendor to provide a printing solution (includes Printing, Scanning, Copying, and Faxing) for bureaus/operating units (B/OUs) at the U.S. Department of Commerce.

SECTION 2. AUTHORITY.

This policy is in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a).

SECTION 3. SCOPE.

This policy applies to all Departmental bureaus and operating units (B/OUs). The Department's B/OUs must ensure privacy compliance for printing, scanning, copying, and faxing of sensitive personally identifiable information (PII) and business identifiable information (BII).

SECTION 4. PRIVACY REQUIREMENTS FOR PRINTING FUNCTIONS.

1. **BASIC PRIVACY REQUIREMENTS FOR PRINTERS**

    a. All shared printers must utilize secure multi-factor authentication (MFA) for secure/follow-me printing.
    b. The printer must have the ability to support encryption for all inbound/outbound communication with the device for printing, scanning or remote management using a combination of secure sockets layer (SSL), Internet Protocol Security (IPSec), Secure Shell (SSH), and/or Internet Printing Protocol (IPP).
    c. All printer encryption must be FIPS 140-2 compliant.
    d. Printers with scan to email functions must encrypt the body of the email and all attachments for the protection of PII/BII.
    e. Printers with the capability to store directly to network device storage must support system user authenticated credentials.
    f. Printers with the capability to store to shared folders must support authorized "need to know" access.
    g. Printers with the capability to scan to USB devices must support encrypted USB devices which require password authentication.

h. All peripheral IT system components transmitting, processing, and storing of government data, including but not limited to printers, multifunction devices, software, and print servers, must comply with FISMA moderate security controls, and shall be subject to regular auditing to ensure compliance. In addition, the information systems must be compliant with all relevant IRS Pub. 1075 security requirements, and are subject to regular IRS Safeguard auditing.

i. Printers must support factory reset capabilities, to include settings in Volatile memory, Non-volatile memory, and Hard disk memory.

2. PRIVACY REQUIREMENTS BY PRINTER FUNCTIONS

The following privacy requirements must be included for devices providing any of the following printer functions below:

a. Printing

i. Must offer secure print services (follow-me printing) which shall allow a user to print to any printer on the network from a shared work queued. Users shall be able to print documents from any printer using MFA.

b. Copying

i. Must provide the capability to copy based on user authenticated credentials.

c. Faxing

i. Must provide the capability to fax based on user authenticated credentials.

d. Scanning

i. Scan to File – Must provide scan to desktop, shared directories, and network storage based upon authenticated user credentials.

ii. Scan to email **–** Must utilize FIPS 140-2 encryption for transmission of the body of the email and attachments.

iii. Scan to USB Device – Must provide the capability to scan to an approved encrypted USB device requiring password authentication.

Appendix D – Categorizing PII

Categorizing Personally Identifiable Information (PII)

This document adopts use of the OMB recommended Best Judgment Standard and follows a twostep approach regarding categorizing information about individuals: (i) consider whether the information is within scope of the definition of PII, and (ii) consider the sensitivity of the PII in the context in which it appears. The sections below facilitate completion of the first step of OMB's approach by identifying PII and PHI.[2] Implementation of the second step of OMB's approach within DOC is discussed below under "Categorizing PII Using NIST SP 800-122 defined Confidentiality Impact Levels."

****IMPORTANT NOTE****
The PII confidentiality impact level is not the same, and should not be confused with, the security objective of confidentiality for the system.

Identifying PII

OMB memoranda collectively define PII as (i) data elements which alone can distinguish or trace an individual's identity, i.e., unique identifiers; (ii) non-PII that becomes PII when it identifies an individual in aggregate, i.e., compilation effect; and (iii) non-PII that becomes PII when combined with a unique identifier or data elements that have aggregated to become PII, i.e., by association.[3] Data elements which meet one or more of these criteria are PII and should be protected.

(i) Data elements which alone can distinguish or trace an individual's identity Many types of data elements can uniquely identify an individual without the need to first combine it with other data elements. This category of PII is most commonly encountered when a

[2] To protect PII within an information system, system owners must be able to locate and identify the PII and should recognize that inclusion of PII in a system may not be immediately apparent. System owners should be familiar with all aspects of an information system. Examples of where PII may be identified for a system include the data dictionary, the architecture for the data store(s), or the data store(s) themselves. For existing systems, current privacy documentation, such as Privacy Impact Assessments (PIAs) and system of records notices (SORNs), may provide insight into the types of PII in a system, but they may be documented at a higher level of categories or types than is necessary for the categorization of system information and determining privacy risk for the purposes of implementing the Privacy Overlays.

[3] See, for example, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, (22 May 2007); OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, (25 June 2010); OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, (25 June 2010).

unique number or other identifier is assigned to an individual (e.g., name,[4] Social Security Number, passport number, or driver's license number) or with respect to unique identifiers that are part of an individual's physical person (e.g., biometrics, such as fingerprints, iris, voice prints, or facial images). These unique identifiers alone can be used to identify a specific individual.

(ii) Non-PII becomes PII when it is combined with other information to identify an individual

Akin to the compilation effect, data elements which alone do not identify an individual and are not PII can become PII if, when combined, they uniquely identify an individual. [5] For example, a zip code, birthdate, or gender alone will not identify someone. However, if these three elements are associated with each other they narrow the scope of reference and enable either identification or re-identification of the individual, thereby making these elements PII.

Accordingly, prevention against re-identification[5] under the compilation effect extends beyond the mere removal of name and social security number. To ensure that information does not compile to become PII, refer to one of the accepted methods of data de-identification such as those prescribed by HIPAA.[6] In the event non-PII compiles into PII, the information system will require re-examination and possible adjustment to the PII confidentiality impact level for that system, possibly invoking use of the Privacy Overlays and other applicable privacy requirements.

(iii) Non-PII becomes PII when combined with a unique identifier or when combined with data elements that have aggregated to become PII

When information that is not otherwise attributed to one individual is associated with PII, then the non-attributable information becomes PII by association. For example, information contained in a financial record of an unidentified individual is not PII,

---

[4] An individual's name alone falls within the definition of PII provided by OMB M-07-16. This is true whether a particular name is unique, such as Glenn Schlarman, or if the name is relatively common, such as John Smith, and additional PII is necessary to successfully distinguish one individual from another. Whether information falls within the definition of PII is a separate evaluation than the sensitivity of that information.

[5] OMB M-10-23, clarifies the definition of PII in the *Definitions* section. ("The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an organization to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.") [5] *Re-identification* refers to the use of a combination of data in a record that has been previously anonymized by the removal of PII to re-establish the identity of the individual.

[6] See Department of Health and Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, available online at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/guidance.html (accessed 28 March 2015).

e.g., purchasing history without any other identifying information. However, if the financial record subsequently is linked or linkable to a name or other unique identifier for a particular individual, e.g., credit card number or account number, then the entire financial record becomes PII, i.e., the buying habits of an individual.

Categorizing PII Using NIST SP 800-122 Defined PII Confidentiality Impact Levels

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, provides guidance on how to categorize the sensitivity of PII resulting in selection of a **PII confidentiality impact level.** The PII confidentiality impact levels in NIST SP 800-122 — low, moderate, or high — are based on a combination of the FIPS 199 impact values and six factors for determining the harm[7] (*see* Table 2 below) that could result to the subject individuals, the organization, or both, if PII were inappropriately accessed, used, or disclosed.[8]

The FIPS 199 impact value definitions are written for information (information types) and information systems and NIST SP 800-122 adopts the "low, moderate, or high" framework for the risk to the PII information type.[9]

The OMB recommended process requires performing a two-step approach to first identify all

---

[7] NIST SP 800-122, Section 3.1, "For the purposes of this document, *harm* means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability."

[8] NIST SP 800-122, Section 3.2, discusses the use of six factors to determine impact levels and the freedom of agencies to determine the most relevant factors, including extending the six factors when appropriate. The six factors include identifiability, quantity of PII, data field sensitivity, context of use, obligation to protect confidentiality, and access to and location of PII (see Table 2 of the Privacy Overlays for illustrative examples of these six factors for each PII confidentiality impact level). NIST SP 800-122 leaves it to the organization's discretion to determine whether additional factors should be considered beyond the six defined by NIST. NIST also notes the importance of considering the relevant factors together as the impact levels of each factor may differ.

[9] FIPS 199, Footnote 1, "Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation." When identifying information types, some data elements may be more easily recognized as PII than others, e.g., social security numbers. NIST SP 800-60, Volume II contains detailed descriptions of information types, including a discussion of which information types are likely to have privacy implications. Some examples of those information types with privacy implications include: Program Evaluation, Travel, Intelligence Operations, Space Operations, and Health Care Administration.

PII in the system and then determine the sensitivity of that PII (alone and then in context) and implement protections commensurate with its sensitivity. Table 1, below, provides the impact values defined in FIPS 199, as incorporated in NIST SP 800-122, which are based on the potential impact of a security breach involving a particular system. *Table 1 should be used in concert with Table 2. Use Table 1 to gain an understanding of the potential adverse effects on individuals, organizational assets, or organizations based on the listed impact value. Use Table 2 to identify the applicable PII confidentiality impact levels based on the factors and illustrative examples of impact descriptions listed.*

Table 1: FIPS 199 Potential Impact Values as Incorporated in NIST SP 800-122

Potential Impact Value	**Type of adverse effect on organizational operations, organizational assets, or individuals**	**Expected adverse effect of the loss of confidentiality, integrity, or availability on organizational operations, organizational assets, or individuals**
LOW	Limited	(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
MODERATE	Serious	(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
HIGH	Severe or catastrophic	(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Table 2 provides six factors described in NIST SP 800-122, with illustrative examples aligned to the three PII confidentiality impact levels.

Table 2: Illustrative Examples of the Six Factors Described in NIST SP 800-122 as Used in Determining PII Confidentiality Impact Levels[10]

NIST SP 800122 Factors	NIST SP 800-122 PII Confidentiality Impact Level[11]		
	Low	**Moderate**	**High**
Identifiability	Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.	Combined data elements uniquely and directly identify individuals.	Individual data elements directly identifying unique individuals.
Quantity of PII	A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.	A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a serious or substantial amount of data.	A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a significantly large amount of data, e.g., "Big Data."
Data Field Sensitivity	Data fields, alone or in combination, have little relevance outside the context.	Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.	Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
Obligation to Protect Confidentiality[12]	Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.	Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide	Organization or Mission specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to governmentwide or industry-specific

[10] These examples are for illustrative purposes and provided to clarify the six factors from NIST SP 800-122; each instance of PII is different, and each organization has a unique set of requirements and different missions to consider.

[11] NIST SP 800-122, p. ES-2, "PII should be evaluated to determine its PII confidentiality impact level, which is different from the Federal Information Processing Standard (FIPS) Publication 199 confidentiality impact [value], so that appropriate safeguards can be applied to the PII. The PII confidentiality impact level — *low*, *moderate*, *or high* — indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed."

[12] NIST SP 800-122, p. ES-3, "An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance). For example, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII." NIST 800-122, Section 3.2.5, advises that "Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization 's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time."

NIST SP 800122 Factors	NIST SP 800-122 PII Confidentiality Impact Level		
	Low	**Moderate**	**High**
		requirements. Violations may result in serious civil or criminal penalties.	requirements. Violations may result in severe civil or criminal penalties.
Access to and Location of PII	Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.	Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at contractor-owned facilities.	Located on computers and other devices on a network not controlled by the organization or on mobile devices or storage media. Access open to the organization's entire workforce. Remote access allowed by equipment owned by others (e.g., personal mobile devices). Information can be stored on equipment owned by others (e.g., personal USB drive).
Context of Use	Disclosure of the act of collecting, and using the PII, *or* the PII itself is unlikely to result in limited harm to the individual or organization such as name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.	Disclosure of the act of collecting, and using the PII, *or* the PII itself may result in serious harm to the individual or organization such as name, address, and phone numbers of a list of people who have filed for retirement benefits.	Disclosure of the act of collecting, and using the PII, *or* the PII itself is likely to result in severe or catastrophic harm to the individual or organization such as name, address, and phone numbers of a list of people who work undercover in law enforcement.

Appendix E – Appendix J Control Allocation Table

Control Types

a. **Common:** Single implementation leveraged and used uniformly across the Department.
b. **Hybrid:** Implementation is split between two or more elements of the Department.
c. **System:** Implementation is unique to the specific system.

ID	Privacy Controls	Identified Control
AP	**Authority and Purpose**	**Control Type**
AP-1	Authority to Collect	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement
AP-2	Purpose Specification	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement
AR	**Accountability, Audit, and Risk Management**	
AR-1	Governance and Privacy Program	**COMMON** – **DEPT Level** – DOO 10-19, DOO 20-31
AR-2	Privacy Impact and Risk Assessment	**SYSTEM** – **System/Program Level** – SORN, PTA/PIA, and PA Statement
AR-3	Privacy Requirements for Contractors and Service Providers	**HYBRID** – **DEPT Level** – CAM 1337.7; DOC Privacy Program Plan **System/Program Level** – Contract Privacy Provisions
AR-4	Privacy Monitoring and Auditing	**HYBRID** – **DEPT Level** – DOC DLP Policy **System/Program Level** – DLP and Privacy Monitoring Tools/ Capabilities
AR-5	Privacy Awareness and Training	**HYBRID** – **DEPT Level** – DOC Privacy Training/ Awareness **System/Program Level** – Bureau/ System Privacy Training/ Awareness
AR-6	Privacy Reporting	**COMMON** – **DEPT Level** –DOC PA, PII, BII Breach Notification Plan, and Annual FISMA/Privacy Reports

ID	Privacy Controls	Identified Control
AR-7	Privacy-Enhanced System Design and Development	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement
AR-8	Accounting of Disclosures	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement
DI	**Data Quality and Integrity**	
DI-1	Data Quality – Hybrid	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement

ID	Privacy Controls	Identified Control
DI-2	Data Integrity and Data Integrity Board	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement
DM	**Data Minimization and Retention**	
DM-1	Minimization of Personally Identifiable Information	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement
DM-2	Data Retention and Disposal	**SYSTEM** – **System/Program Level** – SORN, PIA, and PA Statement, Record Schedule
DM-3	Minimization of PII Used in Testing, Training, and Research	**HYBRID** – **DEPT Level** – DOC Privacy Program Plan **System/Program Level** – SORN, PIA
IP	**Individual Participation and Redress**	
IP-1	Consent	**SYSTEM** – **System/ Program Level** – SORN, PIA, and PA Statement
IP-2	Individual Access	**HYBRID** – **DEPT Level** – SORN and PIA
IP-3	Redress – System level, unless decision made to determine process at enterprise level, then hybrid	**HYBRID** – **DEPT Level** – DOC Privacy Act Handbook **System/Program Level** – SORN, PIA, and PA Statement

ID	Privacy Controls	Identified Control
IP-4	Complaint Management	**HYBRID –** **DEPT Level –** DOC Privacy Act Handbook **System/Program Level –** SORN, PIA, and PA Statement
SE	**Security**	
SE-1	Inventory of Personally Identifiable Information	**HYBRID –** **DEPT Level –** SAOP FISMA Guidance and Reporting **System/Program Level –** SORN, PIA, and PA Statement
SE-2	Privacy Incident Response	**HYBRID–** **DEPT Level –** DOC PA, PII, and BII Breach Notification Plan **System/ Program Level** - CIRT, Breach Response Processes
TR	**Transparency**	
TR-1	Privacy Notice	**SYSTEM –** **System/Program Level –** SORN, PIA, and PA Statement
TR-2	System of Records Notices and Privacy Act Statements	**SYSTEM –** **System/Program Level –** SORN, PIA, and PA Statement

ID	Privacy Controls	Identified Control
TR-3	Dissemination of Privacy Program Information	**COMMON –** **DEPT Level –** DOC Privacy Program Plan and DOC Privacy Website
UL	**Use Limitation**	
UL-1	Internal Use	**SYSTEM –** **System/Program Level –** SORN, PIA, and PA Statement
UL-2	Information Sharing with Third Parties	**SYSTEM –** **System/Program Level –** SORN, PIA, and PA Statement

Appendix F – Implementing Privacy Overlays

Introduction

This document is comprised of four Privacy Overlays that identify security and privacy control specifications required to protect personally identifiable information (PII), including protected health information (PHI), in DOC systems and reduce privacy risks to individuals throughout the information lifecycle.[1] The Privacy Overlays support implementation of but are not intended to, and do not, supersede privacy requirements of statute, regulation, or Office of Management and Budget (OMB) policy.

Since the Privacy Act of 1974 established the requirement for "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" and "to protect… the integrity" of systems, both the technology and threats thereto have evolved and organizations have had to change the way they protect their information.[2] The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 provides the underlying controls necessary to protect PII processing systems within DOC. Based on the Fair Information Practice Principles (FIPPs)[3] and federal privacy requirements, these Privacy Overlays provide a consistent approach for ensuring implementation of "appropriate administrative, technical, and physical safeguards" to protect PII in information systems irrespective of whether the PII is maintained as part of a system of records.[4] The Privacy Overlays provide a method within existing NIST structures to implement the security and privacy controls necessary to protect PII in today's technology-dependent world.

All PII is not equally sensitive and therefore all PII does not require equal protection. PII with higher sensitivity requires more stringent protections, while PII with lower sensitivity requires less stringent protections. There are three overlays that address the varying sensitivity of PII; Low, Moderate, and High. PHI is a subset of PII and in addition to sensitivity considerations, PHI requires a minimum set of protections that are based on the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules. Therefore, PHI is addressed under a fourth overlay, which is applied on top of the Privacy Overlay determined by the sensitivity of the PHI, i.e., Low, Moderate, or High.

---

[1] For additional information about PII and PHI, see Section 7, "Definitions."

[2] "Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any unanticipated 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." 5 U.S.C. §552a(e) (10).

[3] Committee Report No. 93-1183 to accompany S. 3418 (Sep 26, 1974), p 9.

[4] "[A system of records is] a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. §552a(a)(5).

Overlays Summary

The table contains a summary of the security and privacy control specifications as they apply in the Privacy Overlays. The detailed specifications and tailoring considerations for each control can be found in the sections that follow. The symbols used in the table are as follows:

- A plus sign ("+") indicates the control should be selected.
- Two "dashes" ("--") indicates the control should not be selected.[18]
- The letter "E" indicates there is a control extension.[19]
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter "V" indicates this overlay defines a value for an organizational-defined parameter for the control.
- The letter "R" indicates there is at least one regulatory/statutory reference that affects the control selection or that the control helps to meet the regulatory/statutory requirements.

Controls that include an E, G, V, or R specification without a "+" or a "--" are not required, but they do have privacy implications when implemented for other reasons. Please see the Tailoring Considerations section for more information regarding these specifications.

---

[18] AC-2(8) includes regulatory/statutory references that prohibit its selection of this control for systems that maintain PII with a PII Confidentiality Impact Level of Moderate or High and for PHI.

[19] Control extensions will be submitted to NIST for consideration when updating the NIST SP 800-53 catalog.

Table: Privacy Overlays Security and Privacy Controls

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
AC-1	+GR	+GR	+GR	+ER
AC-2	+EGVR	+EGVR	+EGVR	+EGR
AC-2(8)		--R	--R	
AC-2(9)	GVR	GVR	GVR	R
AC-2(13)	+R	+R	+R	+R
AC-3	+EGR	+EGR	+EGR	+GR
AC-3(9)		+EVR	+EVR	+R
AC-3(10)	GVR	GVR	GVR	
AC-4		+GR	+GR	+R
AC-4(8)			+VR	
AC-4(12)				+GR
AC-4(15)		+GR	+GR	+R
AC-4(17)		+GVR	+GVR	
AC-4(18)		+GR	+GR	+R
AC-5		+GR	+GR	+GR
AC-6		+GR	+GR	+GR
AC-6(1)			+GR	+R
AC-6(2)		+GR	+GR	+R
AC-6(3)			GR	
AC-6(5)			+R	+R
AC-6(7)	+VR	+VR	+VR	+VR
AC-6(9)		+R	+R	+R
AC-6(10)		+R	+R	
AC-8	GR	GR	GR	GR
AC-11	+EVR	+EVR	+EVR	+GR
AC-12				+GR
AC-14		GR	GR	GR
AC-16	+GVR	+GVR	+GVR	+GVR
AC-16(3)	+GVR	+GVR	+GVR	+GVR
AC-17	+GR	+GR	+GR	+GR
AC-17(1)	+GR	+GR	+GR	+R
AC-17(2)	+R	+R	+R	+GR
AC-18(1)	+GR	+GR	+GR	
AC-19	+ER	+ER	+ER	+GR

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
AC-19(5)	+EVR	+EVR	+EVR	+GVR
AC-20	+EGR	+EGR	+EGR	+R
AC-20(1)	+R	+R	+R	+R
AC-20(3)	+EGVR	+EGVR	+EGVR	
AC-21	+GR	+GR	+GR	+GR
AC-22	+GR	+GR	+GR	+R
AC-23	EGR	EGR	EGR	
AT-1	+GR	+GR	+GR	+R
AT-2	+ER	+ER	+ER	+GR
AT-3	+ER	+ER	+ER	+R
AT-4	+GR	+GR	+GR	+R
AU-1	+GVR	+GVR	+GVR	+R
AU-2	+GVR	+GVR	+GVR	+GR
AU-3	+GR	+GR	+GR	+R
AU-4		+GR	+GR	+R
AU-4(1)		GR	GR	R
AU-6		+GR	+GR	+R
AU-6(3)		+R	+R	
AU-6(10)		+GR	+GR	
AU-7	+R	+R	+R	+R
AU-7(1)		+R	+R	+R
AU-7(2)		+R	+R	+R
AU-9	+GR	+GR	+GR	+R
AU-9(3)		+GR	+GR	+GR
AU-9(4)		GR	GR	
AU-10		+GR	+GR	+R
AU-10(1)		+GR	+GR	+R
AU-11(1)		GR	GR	
AU-12		+R	+R	+R
AU-12(3)		+VR	+VR	+VR
AU-14		GR	GR	
AU-14(2)		GR	GR	
AU-14(3)		GR	GR	
AU-16(2)				+GVR
CA-1	+GR	+GR	+GR	+R

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
CA-2	+GR	+GR	+GR	+VR
CA-3		+R	+R	+GVR
CA-3(3)	+VR	+VR	+VR	+R
CA-3(5)	+VR	+VR	+VR	+R
CA-6	+EGR	+EGR	+EGR	+GR
CA-7		+GR	+GR	+GR
CA-8			+GVR	
CA-9		+GVR	+GVR	+VR
CA-9(1)		+GR	+GR	+R
CM-3(6)	+GVR	+GVR	+GVR	+GVR
CM-4	+GR	+GR	+GR	+R
CM-4(1)		+GR	+GR	
CM-4(2)		+R	+R	+R
CM-8(1)				+R
CP-1	+R	+R	+R	+R
CP-2	+R	+R	+R	+GR
CP-2(5)				+R
CP-2(8)				+GR
CP-4				+GR
CP-7		GR	GR	GVR
CP-9		+ER	+ER	+ER
CP-10		+R	+R	+R
IA-2	+R	+R	+R	+R
IA-2(6)		+GR	+GR	
IA-2(7)		+GR	+GR	
IA-2(11)		+GR	+GR	
IA-3				+R
IA-4	+ER	+ER	+ER	+GR
IA-4(3)		+GR	+GR	
IA-5		+R	+R	+GR
IA-6				+GR
IA-7	+GR	+GR	+GR	+GR
IA-8		+R	+R	+R
IR-1	+GVR	+GVR	+GVR	+GR
IR-2	+GR	+GR	+GR	+GR

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
IR-4	+GR	+GR	+GR	+GR
IR-4(3)				+EVR
IR-5	+GR	+GR	+GR	+R
IR-6	+GVR	+GVR	+GVR	+R
IR-7	+GR	+GR	+GR	+R
IR-8	+GR	+GR	+GR	+GR
IR-10	+GR	+GR	+GR	
MA-1		+ER	+ER	+GR
MA-2				+GR
MA-4(6)	+R	+R	+R	+R
MA-5	+GR	+GR	+GR	+GR
MP-1	+VR	+VR	+VR	+VR
MP-2	+VR	+VR	+VR	+VR
MP-3	+GR	+GR	+GR	+GR
MP-4	+VR	+VR	+VR	+R
MP-5	+VR	+VR	+VR	+VR
MP-5(4)	+R	+R	+R	+GR
MP-6		+GVR	+GVR	+VR
MP-6(1)	+GR	+GR	+GR	+GR
MP-6(8)		+GR	+GR	
MP-7		+GVR	+GVR	
MP-7(1)		+R	+R	
MP-8(3)		+VR	+VR	+GVR
PE-1				+R
PE-2	+R	+R	+R	+GR
PE-2(1)				+GR
PE-3	+R	+R	+R	+R
PE-4				+GR
PE-5	+GR	+GR	+GR	+GR
PE-6				+GR
PE-8				+GR
PE-17	+GR	+GR	+GR	
PE-18			+GR	+GR
PL-1				+ER
PL-2	+EGR	+EGR	+EGR	+R

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
PL-4	+ EGR	+EGR	+EGR	
PL-8	+GR	+GR	+GR	
PS-1	+ER	+ER	+ER	+R
PS-2	+ER	+ER	+ER	+GR
PS-3	+ER	+ER	+ER	+GR
PS-3(3)	+GVR	+GVR	+GVR	+GR
PS-4	+GR	+GR	+GR	+GR
PS-5	+ER	+ER	+ER	+GR
PS-6	+GR	+GR	+GR	+R
PS-7	+GR	+GR	+GR	+R
PS-8	+EGR	+EGR	+EGR	+R
RA-1	+EGR	+EGR	+EGR	+R
RA-2	+ER	+ER	+ER	+R
RA-3	+EGVR	+EGVR	+EGVR	+GVR
SA-2	+ER	+ER	+ER	
SA-3	+GR	+GR	+GR	
SA-4	+EGR	+EGR	+EGR	+ER
SA-8	+GR	+GR	+GR	
SA-9				+ER
SA-9(5)	+EGR	+EGR	+EGR	
SA-11		+EGR	+EGR	
SA-11(5)			+ER	
SA-15(9)		+EGR	+EGR	
SA-17	+EGR	+EGR	+EGR	
SA-21	+GVR	+GVR	+GVR	+GR
SC-2		+ER	+ER	+ER
SC-4	+GR	+GR	+GR	+R
SC-7(14)				+GVR
SC-8	+GVR	+GVR	+GVR	+VR
SC-8(1)	+EVR	+EVR	+EVR	+GR
SC-8(2)		+GVR	+GVR	
SC-12	+VR	+VR	+VR	+GR
SC-13	+VR	+VR	+VR	+GR
SC-28	+GVR	+GVR	+GVR	+R
SC-28(1)	+EGR	+EGR	+EGR	+GR

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
SI-1	+R	+R	+R	+R
SI-3				+GR
SI-4	+GR	+GR	+GR	+R
SI-5				+GR
SI-7	+VR	+VR	+VR	+VR
SI-7(6)	+ER	+ ER	+ ER	+ GR
SI-8				+ GR
SI-10		+VR	+ VR	
SI-11	+VR	+ VR	+ VR	+ VR
SI-12	+EGR	+EGR	+EGR	+EGR
PM-1	+GR	+GR	+GR	+R
PM-2	GR	GR	GR	+ER
PM-3	+R	+R	+R	
PM-5	+GR	+GR	+GR	+GR
PM-7	+GR	+GR	+GR	+R
PM-9	+ER	+ER	+ER	+ER
PM-10	+EGR	+EGR	+EGR	+ER
PM-11	+EGR	+EGR	+EGR	+R
PM-12	+ER	+ER	+ER	
PM-13	GR	GR	GR	R
PM-14	+EGR	+EGR	+EGR	
PM-15	+EGR	+EGR	+EGR	
AP-1	+GR	+GR	+GR	
AP-2	+GR	+GR	+GR	
AR-1	+EGR	+EGR	+EGR	+GR
AR-2	+GR	+GR	+GR	+R
AR-3	+ER	+ER	+ER	+ER
AR-4	+GVR	+GVR	+GVR	+R
AR-5	+EGR	+EGR	+EGR	+R
AR-6	+R	+R	+R	+GR
AR-7	+GR	+GR	+GR	+R
AR-8	+R	+R	+R	+GR
DI-1	+GR	+GR	+GR	
DI-1(1)		+GR	+GR	
DI-1(2)		+VR	+VR	

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
DI-2	GR	GR	GR	
DI-2(1)	GR	GR	GR	
DM-1	+GR	+GR	+GR	+R
DM-2	+VR	+VR	+VR	+VR
DM-2(1)				+R
DM-3	+GR	+GR	+GR	+GR
DM-3(1)	GR	GR	GR	+GR
IP-1	+GR	+GR	+GR	+GR
IP-1(1)				+R
IP-2	+GR	+GR	+GR	+ER
IP-3	+GR	+GR	+GR	+R
IP-4	+R	+R	+R	+R
IP-4(1)	GR	GR	GR	+R
SE-1	+GR	+GR	+GR	+ R
SE-2	+GR	+GR	+GR	+R
TR-1	+GR	+GR	+GR	+GR
TR-1(1)	G	G	G	GR
TR-2	+GR	+GR	+GR	
TR-2(1)	+GR	+GR	+GR	
TR-3	+R	+R	+R	
UL-1	+EGR	+ EGR	+ EGR	+R
UL-2	+ EGR	+ EGR	+ EGR	+ GR

Privacy Overlay

Appendix G – Privacy Threshold Analysis (PTA) Template

U.S. Department of Commerce
[Bureau Name]

Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information 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)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "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 can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: (*Check all that apply.)*

____ Companies
____ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to 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..."

____ Yes, the IT system collects, maintains, or disseminates PII about: (*Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

_____

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Appendix H – PTA Forms Template

U.S. Department of Commerce
[Bureau Name]

Privacy Threshold Analysis
for the
[Name of Information Collection or Form]

Privacy Threshold Analysis (PTA)

Specialized Template for
Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number:	**Click here to enter text.**		
Form Title:	**Click here to enter text.**		
Component:	Click here to enter text.	Office:	Click here to enter text.

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	**Click here to enter text.**		
OMB Control Number:	Click here to enter text.	OMB Expiration Date:	Click here to enter a date.
Collection status:	Choose an item.	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	**Click here to enter text.**		
Office:	Click here to enter text.	Title:	Click here to enter text.
Phone:	Click here to enter text.	Email:	Click here to enter text.

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	**Click here to enter text.**		
Office:	Click here to enter text.	Title:	Click here to enter text.
Phone:	Click here to enter text.	Email:	Click here to enter text.

SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form
a. Describe the purpose of the information collection or form. ***Please provide a general description of the project and its purpose, including how it supports the DOC mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).*** ***If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.***
Click here to enter text.
b. List the DOC (or component) authorities to collect, store, and use this information. ***If this information will be stored and used by a specific DOC component, list the component-specific authorities.***
Click here to enter text.

2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information" (PII[10])?	☐ Yes ☐ No
b. From which type(s) of individuals does this form collect information? (*Check all that apply*.)	☐ Members of the public ☐ U.S. citizens or lawful permanent residents ☐ Non-U.S. Persons. ☐ DOC Employees ☐ DOC Contractors ☐ Other federal employees or contractors.
c. Who will complete and submit this form? (*Check all that apply*.)	☐ The record subject of the form (e.g., the individual applicant). ☐ Legal Representative (preparer, attorney, etc.). ☐ Business entity. If a business entity, is the only information collected business contact information? ☐ Yes ☐ No ☐ Law enforcement.

10 Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

	☐ DOC employee or contractor. ☐ Other individual/entity/organization **that is NOT the record subject**. *Please describe*. Click here to enter text.
d. How do individuals complete the form? *Check all that apply.*	☐ Paper. ☐ Electronic. (ex: fillable PDF) ☐ Online web form. (available and submitted via the internet) *Provide link:*

e. What information will DOC collect on the form? *List all PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.*

Click here to enter text.

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

☐ **Social Security number**	☐ Social Media Handle/ID
☐ **Alien Number (A-Number)**	☐ Known Traveler Number
☐ **Tax Identification Number**	☐ Trusted Traveler Number (Global Entry, Pre-Check, etc.)
☐ **Visa Number**	☐ Driver's License Number
☐ **Passport Number**	☐ Biometrics
☐ **Bank Account, Credit Card, or other financial account number**	
☐ **Other. *Please list:***	

g. List the *specific authority* to collect SSN or these other SPII elements.

Click here to enter text.

h. How will this information be used? What is the purpose of the collection? Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

Click here to enter text.

i. Are individuals provided notice at the time of collection by DOC (*Does the records subject have notice of the collection or is form filled out by third party*)?	☐ Yes. Please describe how notice is provided. Click here to enter text. ☐ No.

3. How will DOC store the IC/form responses?	
a. How will DOC store the original, completed IC/forms?	☐ Paper. Please describe. Click here to enter text. ☐ Electronic. Please describe the IT system that will store the data from the form. Click here to enter text. ☐ Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Click here to enter text.
b. If electronic, how does DOC input the responses into the IT system?	☐ Manually (data elements manually entered). Please describe. Click here to enter text. ☐ Automatically. Please describe. Click here to enter text.
c. How would a user search the information submitted on the forms, *i.e.*, how is the information retrieved?	☐ By a unique identifier.[11] *Please describe*. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. Click here to enter text. ☐ By a non-personal identifier. *Please describe*. Click here to enter text.
d. What is the records retention schedule(s)? *Include the records schedule number.*	Click here to enter text.
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	Click here to enter text.
f. Is any of this information shared outside of the original program/office? *If yes, describe where (other offices or DOC components or external entities) and why. What are the authorities of the receiving party?*	
☐ Yes, information is shared with other DOC components or offices. Please describe. **Click here to enter text.**	

11 Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

☐ **Yes, information is shared *external* to DOC with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe.**
Click here to enter text.

☐ **No. Information on this form is not shared outside of the collecting office.**

Please include <u>a copy of the referenced form and Privacy Act Statement</u> (if applicable) with this PTA upon submission.

Appendix I – Privacy Impact Assessement (PIA) Template

U.S. Department of Commerce
[Bureau Name]

Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
d. Conversions		d. Significant Merging		h. New Interagency Uses	
e. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
f. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name		g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number		g. Salary	
b. Job Title		e. Email Address		h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	

For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	

Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

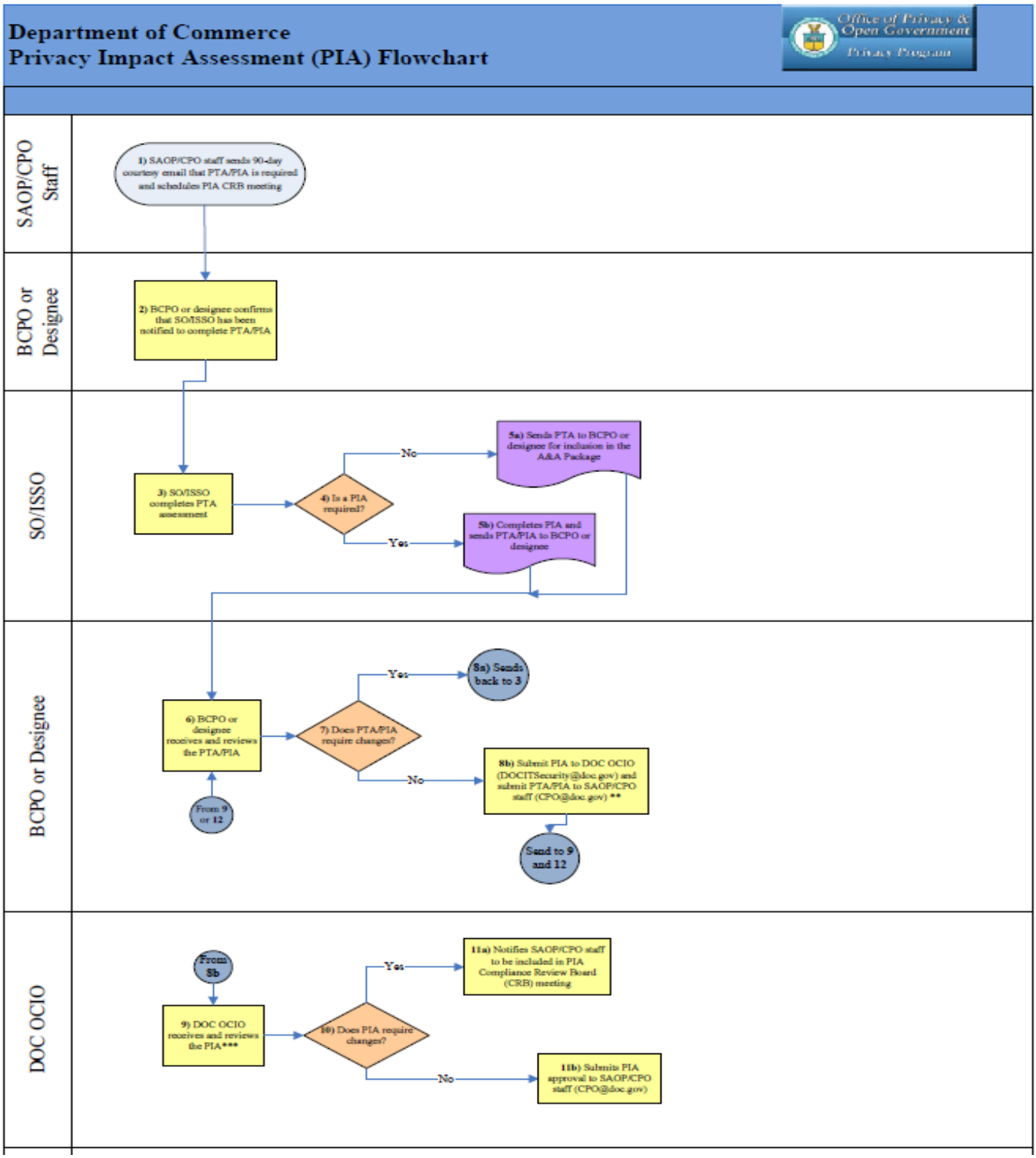
	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

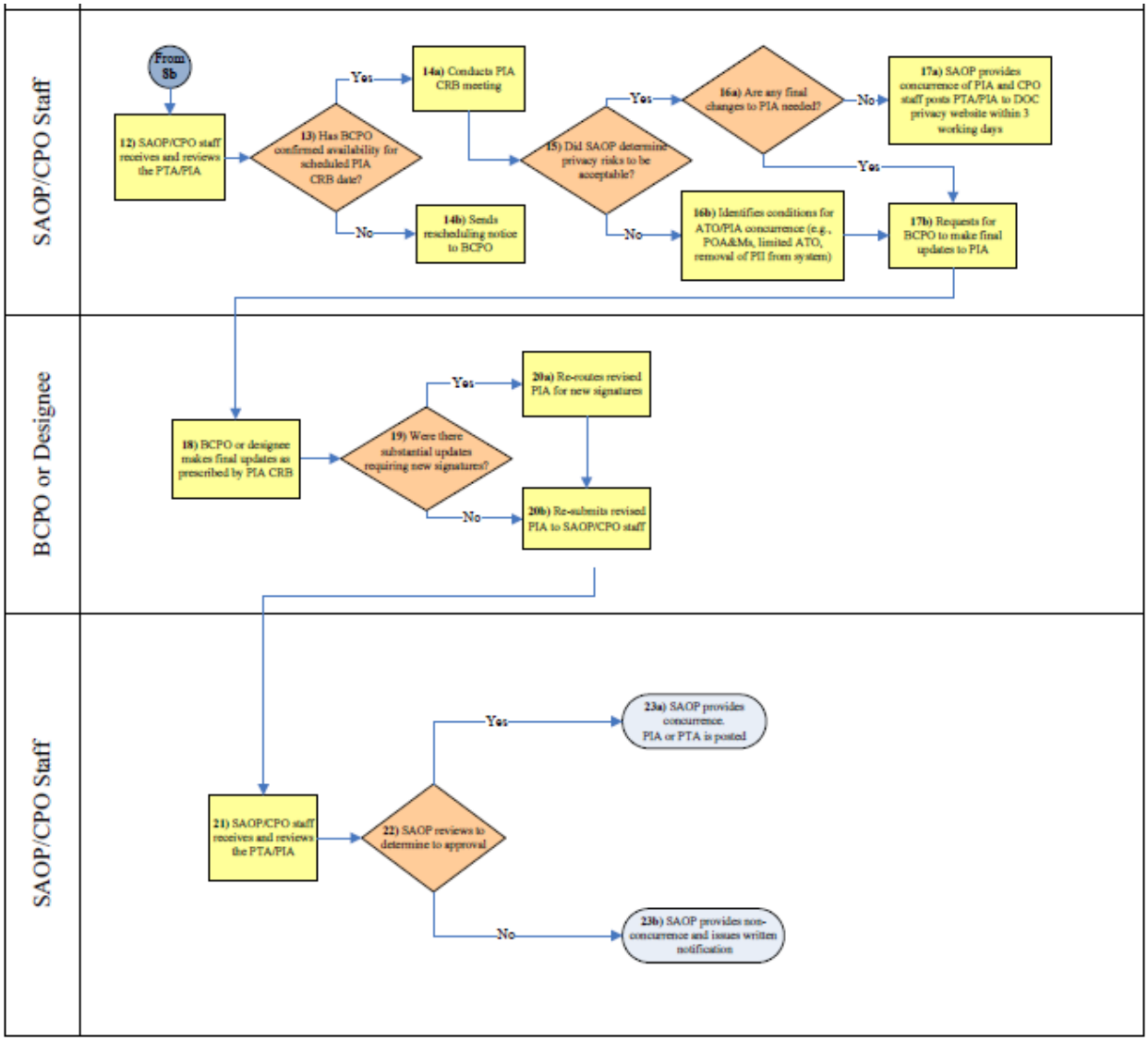
Points of Contact and Signatures

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name: Office: Phone: Email: I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature _____ Date signed: _____	Name: Office: Phone: Email: I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____
Authorizing Official	**Bureau Chief Privacy Officer**
Name: Office: Phone: Email: I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____	Name: Office: Phone: Email: I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: _____ Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Appendix J – Privacy Impact Assessment Flowchart




SAOP/CPO Staff
From 8b
12) SAOP/CPO staff receives and reviews the PTA/PIA
13) Has BCPO confirmed availability for scheduled PIA CRB date?
Yes
14a) Conducts PIA CRB meeting
No
14b) Sends rescheduling notice to BCPO
15) Did SAOP determine privacy risks to be acceptable?
Yes
16a) Are any final changes to PIA needed?
No
17a) SAOP provides concurrence of PIA and CPO staff posts PTA/PIA to DOC privacy website within 3 working days
Yes
No
16b) Identifies conditions for ATO/PIA concurrence (e.g., POA&Ms, limited ATO, removal of PII from system)
17b) Requests for BCPO to make final updates to PIA
BCPO or Designee
18) BCPO or designee makes final updates as prescribed by PIA CRB
19) Were there substantial updates requiring new signatures?
Yes
20a) Re-routes revised PIA for new signatures
No
20b) Re-submits revised PIA to SAOP/CPO staff
SAOP/CPO Staff
21) SAOP/CPO staff receives and reviews the PTA/PIA
22) SAOP reviews to determine to approval
Yes
23a) SAOP provides concurrence. PIA or PTA is posted
No
23b) SAOP provides non-concurrence and issues written notification

Appendix K – PIA Compliance Review Board (CRB) Risk Analysis Guide

PIA CRB
Risk Analysis Guide
(Date of Meeting)

Name of IT System:
Authorization to Operate (ATO) date:
ATO expiration date:

A Privacy Threshold Analysis (PTA) must be completed for a system processing PII/BII in order to determine if a Privacy Impact Assessment (PIA) is required. The purposes of a PIA are to ensure effective compliance with the Privacy Act for notice and disclosure and to confirm appropriate privacy protections are in place. The following critical areas will be discussed during this meeting:

- System/Data characterization
  - System location/Status
  - Type/Sources of information
  - Purpose/Use of information
  - Retention of information
  - Legal authority
  - FIPS 199 security impact category
  - Notice and consent
  - Records retrieval
  - System of records notice(s)
  - NIST SP 800-122 PII confidentiality impact level
- Information Sharing Practices
  - Access
  - Computer Matching Program
  - Connection with other IT systems
- Website/Mobile application processes
  - Website(s)
  - Website privacy policy/Privacy Act statement
  - Mobile application(s)
  - Tracking technologies
- Status of privacy controls
  - Plan of Action and Milestones
  - IT Security controls
- Risk Assessment Review
  - Threats and vulnerabilities
  - Summary risk

Appendix L – PIA Annual Review Certification Form

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: _____

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: _____

Name of Information System Security Officer: _____

Name of Authorizing Official(s): _____

Date of Last PIA Compliance Review Board (CRB): _____
(This date must be within three (3) years.)

Date of PIA Review: _____

Name of Reviewer: _____

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

Appendix M – New/Modified System of Records Notice (SORN) Template

Billing Code:

DEPARTMENT OF COMMERCE

Docket No.

Privacy Act of 1974; System of Records

AGENCY: [Name of agency and, if applicable, agency component].

ACTION: Notice of a [New/Modified] System of Records.

SUMMARY: [A plain-language description of the system]. In accordance with the Privacy Act of 1974 and the Office of Management and Budget (OMB) Circular A 108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," the Department of Commerce (Department) is issuing this notice of its intent to [create/amend] the system of records under [system number, name, e.g., "COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records."]

DATES: To be considered, written comments must be submitted on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. This new/amended system of records will become effective on [INSERT DATE OF PUBLICATION IN *THE FEDERAL REGISTER*], unless the [new/modified] system of records notice needs to be changed as a result of public comment.

Newly proposed routine uses [insert routine uses, if any] in the paragraph entitled "ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES" will become effective on [INSERT DATE 45

DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], unless the [new/modified] system of records notice needs to be changed as a result of public comment. If the [new/modified] system of records notice needs to be changed, the Department will publish a subsequent notice in the *FEDERAL REGISTER* by [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], stating that the current system of records will remain in effect until a revised notice is published in the *FEDERAL REGISTER*.

ADDRESSES: [Instructions for submitting comments on the proposal, including an email address or a website where comments can be submitted electronically].

FOR FURTHER INFORMATION CONTACT: [Instructions for submitting general questions about the system].

SUPPLEMENTARY INFORMATION: [Background information about the proposal, including a description of any changes being made to the system and the purpose(s) of the changes]. The changes are needed because the existing notice for this system of records has not been amended since 2007 and is not up-to-date, accurate, and current, as required by the Privacy Act, 5 U.S.C. 552a (e)(4). This section further provides that OMB Circular A-108 requires agencies to periodically review systems of records notices for accuracy and completeness, paying special attention to changes in the manner in which records are organized, indexed or retrieved that results in a change in the nature or scope of these records. When any of the aforementioned changes occur, the Privacy Act requires agencies to publish in the Federal Register upon revision of a system of records, a notice that describes the amendments to the system of records.

The Privacy Act also requires each agency that proposes to establish or significantly modify a system of records to provide adequate advance notice of any such proposal to the Office of Management and Budget (OMB), the Committee on Oversight and Government Reform of the

House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate (5 U.S.C 552a(r)). Significant modifications include adding a new routine use. The purpose of providing the advance notice to OMB and Congress is to permit an evaluation of the potential effect of the proposal on the privacy and other rights of individuals. The Department filed a report describing the new/amended system of records covered by this notice with the Chair of the Senate Committee on Homeland Security and Governmental Affairs, the Chair of the House Committee on Oversight and Government Reform, and the Deputy Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), on [insert date of letters].

SYSTEM NAME AND NUMBER: [A name for the system that is unambiguous and clearly identifies the purpose or character of the system, and the number of the system].

SECURITY CLASSIFICATION: [An indication of whether any information in the system is classified].

SYSTEM LOCATION: [The address of the agency and/or component responsible for the system, as well as the address of any third-party service provider].

SYSTEM MANAGER(S): [The title, business address, and contact information of the agency official who is responsible for the system].

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: [The specific authority that authorizes the maintenance of the records in the system].

PURPOSE(S) OF THE SYSTEM: [A description of the agency's purpose(s) for maintaining the system].

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: [The categories of individuals on whom records are maintained in the system].

CATEGORIES OF RECORDS IN THE SYSTEM: [The categories of records maintained in the system and, if practicable and useful for public notice, specific data elements].

RECORD SOURCE CATEGORIES: [The categories of sources of records in the system].

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: [Each routine use of the records contained in the system, including the categories of users and the purpose of such use].

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: [The policies and practices of the agency regarding the storage of records].

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: [The policies and practices of the agency regarding retrieval of records].

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: [The policies and practices of the agency regarding retention and disposal of records].

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: [A description of the administrative, technical, and physical safeguards to which the system is subject].

RECORD ACCESS PROCEDURES: [The agency procedures whereby an individual can be notified at his or her request how he or she can gain access to any record pertaining to him or her in the system].

CONTESTING RECORD PROCEDURES: [The agency procedures whereby an individual can be notified at his or her request how he or she can contest the content of any record pertaining to him or her in the system].

NOTIFICATION PROCEDURES: [The agency procedures whereby an individual can be notified at his or her request if the system contains a record pertaining to him or her].

EXEMPTIONS PROMULGATED FOR THE SYSTEM: [Any Privacy Act exemptions promulgated for the system].

HISTORY: [Citation(s) to the last full *Federal Register* notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision].

Dated:

Michael J. Toland
Department of Commerce
Deputy Chief FOIA Officer
Department Privacy Act Officer

Appendix N – Rescindment of a SORN Template

Billing Code:

DEPARTMENT OF COMMERCE

Docket No.

Privacy Act of 1974; System of Records

AGENCY: [Name of agency and, if applicable, agency component].

ACTION: Rescindment of a System of Records Notice.

SUMMARY: [A plain-language description of the system]. In accordance with the Privacy Act of 1974 and the Office of Management and Budget (OMB) Circular A 108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," the Department of Commerce (Department) is issuing this notice of its intent to [create/amend] the system of records under [system number, name, e.g., "COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records."]

DATES: [The date on which the agency stopped or will stop maintaining the system of records].

ADDRESSES: [Instructions for submitting comments on the proposal, including an email address or a website where comments can be submitted electronically].

FOR FURTHER INFORMATION CONTACT: [Instructions for submitting general questions about the system].

SUPPLEMENTARY INFORMATION: [Background information about the proposal, including an account of what will happen to the records that were previously maintained in the system and references to any other SORN that will pertain to the records].

SYSTEM NAME AND NUMBER: [A name for the system that is unambiguous and clearly identifies the purpose or character of the system, and the number of the system].

HISTORY: [Citation(s) to the last full *Federal Register* notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision].

Dated:

Michael J. Toland
Department of Commerce
Deputy Chief FOIA Officer
Department Privacy Act Officer

Appendix O – Summary Incident Report

PII Breach Documentation Form Date:

GENERAL INFORMATION	
Incident Number:	Bureau CIRT Number: U.S. CERT Number:
Office/Division or Location of Incident:	
Date Incident Occurred	
Name of person who reported breach:	
INCIDENT	
Description of incident (what happened):	*Provide the details in order for the Privacy Task Force to understand what actually occurred; include background information if needed.*
Items Breached:	*Example: SSN, DOB, POB, performance ratings, etc.*
Number of People Affected (including internal or external):	*Example: 2 external*
Risk Level	*Answer will be moderate risk, high risk, or major.*
Controls Enabled at Time of Incident (e.g., full-disk encryption, password protection, etc.)	*State "none" if applicable.*

APPROACH TO COMPLIANCE	
Corrective Action(s):	1. *Number each corrective action; begin each action with a present tense verb; example: Complete training in the Commerce Learning Center entitled "How to Protect Personally Identifiable Information (PII) and Business Identifiable Information (BII)."* 2. 3.

PII Breach Documentation Form Date:

SCHEDULE FOR COMPLIANCE	
Date(s) Corrective Action Implemented:	1. *Include the date each corrective action above is completed; example: January 1, 2017* 2. 3.
CONTACT PERSON(S) FOR FOLLOW-UP	
Bureau Chief Privacy Officer Name and Telephone Number:	
DOC Senior Agency Official for Privacy/Chief Privacy Officer Name and Telephone Number:	