Version Number: 01-2015

# U.S. Department of Commerce
# [Bureau Name]

## Privacy Impact Assessment
## for the
## [IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ 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] – AR-2 (review of this and related documents)

**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)*** *a general description of the information in the system –* ***AP-2, see also Section 5.1***

*(b) a description of a typical transaction conducted on the system*

*(c) any information sharing conducted by the system*

***(d)*** *a citation of the legal authority to collect PII and/or BII –* ***AP-1***

*(e) the Federal Information Processing Standard (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)** | | | | | |
|---|---|---|---|---|---|
| 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.

## Section 2: Information in the System – DM-1, UL-1

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) – UL-1** | | | | | |
|---|---|---|---|---|---|
| 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): DM-3 if used for testing and training | | | | | |

| **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.)* DI-1

| **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 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 - AP-2, DI-1

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

| **Purpose** | | | |
|---|---|---|---|
| To determine eligibility | | 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 – AP-2, DI-1, DM-3

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).

## Section 6: Information Sharing and Access - AR-8; UL-2

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.<br>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 – IP-1

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

| | | |
|---|---|---|
| TR-2 | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. | |
| TR-2 | 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. – IP2; IP3

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

| | | |
|---|---|---|
| | opportunity to review/update PII/BII pertaining to them. | |

## Section 8: Administrative and Technological Controls

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

| | |
|---|---|
| AR-3 | All users signed a confidentiality agreement or non-disclosure agreement. |
| AR-3 | All users are subject to a Code of Conduct that includes the requirement for confidentiality. |
| AR-5 | Staff (employees and contractors) received training on privacy and confidentiality policies and practices. |
| AR-3 | Access to the PII/BII is restricted to authorized personnel only. |
| AR-3 | Access to the PII/BII is being monitored, tracked, or recorded.<br>Explanation: |
| AR-4 | The information is secured in accordance with FISMA requirements.<br>Provide date of most recent Assessment and Authorization (A&A): _____<br>☐ 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. |
| AR-4, DI-2 | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). |
| AR-3 | 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. – AR-4, DI-2

| |
|---|
| |

## Section 9: Privacy Act – TR-2

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).<br>Provide the SORN name and number *(list all that apply)*: |
| | Yes, a SORN has been submitted to the Department for approval on (date). |
| | No, a SORN is not being created. |

## Section 10: Retention of Information – DM-2

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.<br>Provide the name of the record control schedule: |
| | No, there is not an approved record control schedule.<br>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 Levels

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.

| | |
|---|---|
| | 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 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.<br>Explanation: |
| | No, the conduct of this PIA does not result in any required business process changes. |

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

| | |
|---|---|
| | Yes, the conduct of this PIA results in required technology changes.<br>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:<br>Office:<br>Phone:<br>Email:<br><br>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.<br><br>Signature: _____<br><br>Date signed: _____ | Name:<br>Office:<br>Phone:<br>Email:<br><br>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.<br><br>Signature: _____<br><br>Date signed: _____ |
| **Authorizing Official** | **Bureau Chief Privacy Officer** |
| Name:<br>Office:<br>Phone:<br>Email:<br><br>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.<br><br>Signature: _____<br><br>Date signed: _____ | Name: Mark Graff<br>Office: NOAA OCIO<br>Phone: 301-628-5658<br>Email: mark.graff@noaa.gov<br><br>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.<br><br>Signature: _____<br><br>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.**