Template Version Number: 01-2020

# U.S. Department of Commerce
# Office of the Secretary

## Privacy Impact Assessment
## for the
## Network C General Support System (GSS)

Reviewed by: Maria D. Dumas, 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

Tahira Murphy for/Jennifer Goode 5/11/2022

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

# U.S. Department of Commerce Privacy Impact Assessment
# Office of the Secretary/Network C

**Unique Project Identifier: Network C**

**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*

Network C is a General Support System (GSS).

*(b) System location*

Network C is located at the Department of Commerce (DOC) Herbert C. Hoover Building (HCHB) in Washington DC.

*(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

Network C hosts various major applications used by DOC Bureaus charged with missions that support the National Essential Functions (NEF). The Network C GSS network is used by the Office of the Secretary (OS), Office of Security (OSY), the Bureau of Industry and Security (BIS), the International Trade Administration (ITA), the National Institute of Standards and Technology (NIST), the National Oceanic and Atmospheric Administration (NOAA), the National Telecommunication and Information Administration (NTIA), and the Office of the Chief Information Officer (OCIO).

*(d) The way the system operates to achieve the purpose(s) identified in Section 4*

Network C obtains its external connectivity from Defense Intelligence Agency (DIA) Joint Worldwide Intelligence Communications System (JWICS). The purpose of Network C GSS is for the hosting applications to be able to transmit, receive, and store classified information up to Top Secret/Sensitive Compartmented Information (TS/SCI).

*(e) How information in the system is retrieved by the user*

Network C GSS users are required to log in using their authenticated credentials (username and password) to gain network connectivity. For users to access the INTELINK extranet to exchange information they must log in utilizing a soft token.

*(f) How information is transmitted to and from the system*

Network C GSS users transmit data to and from the system by utilizing INTELINK to read, write and transfer data. The data processed within the Network C GSS environment is transmitted via the TACLANE encrypted devices to protect the data from being read and or intercepted while in transit.

*(g) Any information sharing conducted by the system*

Network C GSS utilizes INTELINK for information sharing with other agencies.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

15 U.S.C. 1501 et. seq.; 44 U.S.C. 3101 (Records Management); 5 U.S.C. 301 (Departmental Regulations); 5 U.S.C. 7311 (Suitability, Security, and Conduct); 5 U.S.C. 7531-33 (Adverse Actions, Suspension and Removal, and Effect on Other Statutes); Executive Order 10450 (Security Requirements for Government Employment); Executive Order 13526 and its predecessor orders (Classified National Security Information); Executive Order 12968 (Access to Classified Information); HSPD-12, 8/27/04 (Homeland Security Presidential Directive); Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans); Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information); Public Law 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004); Intelligence Authorization Act for FY 2010, Public Law 111-259; Title 50 U.S.C. 402a, Coordination of Counterintelligence Activities; Executive Order 12829 (National Industrial Security Program); Committee for National Security System Directive 505 (Supply Chain Risk Management); Presidential Memorandum National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Program.

*(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

Network C GSS has been categorized as a High impact level 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, and there is not a SAOP approved Privacy Impact Assessment.

____ 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 01-2017).

__X__ 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 01-2019 or later).

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

| **General Personal Data (GPD)** | | | | | |
|---|---|---|---|---|---|
| a. Name | X | h. Date of Birth | X | o. Financial Information | |
| b. Maiden Name | | i. Place of Birth | | p. Medical Information | |
| c. Alias | | j. Home Address | X | q. Military Service | |
| d. Gender | | k. Telephone Number | X | r. Criminal Record | |
| e. Age | | l. Email Address | X | s. Physical Characteristics | |
| f. Race/Ethnicity | | m. Education | | t. Mother's Maiden Name | |
| g. Citizenship | | n. Religion | | | |
| u. Other general personal data (specify): | | | | | |

| **Work-Related Data (WRD)** | | | | | |
|---|---|---|---|---|---|
| a. Occupation | X | e. Work Email Address | X | i. Business Associates | |
| b. Job Title | X | f. Salary | | j. Proprietary or Business Information | |
| c. Work Address | X | g. Work History | | k. Procurement/contracting records | |
| d. Work Telephone Number | X | h. Employment Performance Ratings or | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | other Performance Information | | | |
| l. Other work-related data (specify): | | | | | |

| **Distinguishing Features/Biometrics (DFB)** | | | | | |
|---|---|---|---|---|---|
| a. Fingerprints | | f. Scars, Marks, Tattoos | | k. Signatures | |
| b. Palm Prints | | g. Hair Color | | l. Vascular Scans | |
| c. Voice/Audio Recording | | h. Eye Color | | m. DNA Sample or Profile | |
| d. Video Recording | | i. Height | | n. Retina/Iris Scans | |
| e. Photographs | | j. Weight | | o. Dental Profile | |
| p. Other distinguishing features/biometrics (specify): | | | | | |

| **System Administration/Audit Data (SAAD)** | | | | | |
|---|---|---|---|---|---|
| a. User ID | X | c. Date/Time of Access | X | e. ID Files Accessed | X |
| b. IP Address | X | f. Queries Run | X | f. Contents of Files | X |
| 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 | X |
| 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.

NS3 ensures security protocols and industry best practices are performed regularly to maintain data integrity. NS3 has multiple system security controls in place and performs the following functions to ensure data integrity.

1. Review and update data on a regular basis
2. Use reliable data resources
3. Ensure the reliability and credibility of the data prior to input into the system
4. Standardize data definitions
5. Perform and use error checking and data validation (restricted invalid data values being entered into system)
6. Need to know access to data (Privilege Access)
7. Access to data based on Role-Base Access for Personnel
8. Multi-factor authentication for system access to data
9. Archive Regularly
10. Verify protocols address data quality and reliability

The technologies used to protect PII/BII on System C include but not limited to the following:

1. Managed boundary protection mechanisms (Firewalls, Routers, Switches, and Encryption Devices such as TACLANE) isolate systems from outsiders and other DOC systems
2. Least privilege access controls using group policy and Active Directory
3. Vulnerability scans are executed weekly to identify vulnerabilities, system software and assess system weaknesses.

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection. |
| X | 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): Soft tokens are used to access the INTELINK extranet to exchange information. | | | |

| | |
|---|---|
| X | 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): | | | |

| | |
|---|---|
| X | 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 | X | To promote information sharing initiatives | |
| For litigation | X | For criminal law enforcement activities | X |
| For civil enforcement activities | X | For intelligence activities | X |
| 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).

NS3 is a Trusted Agent (TA) for issuing PIV credentials and has access to the DoD system Defense Enrollment Eligibility Reporting System to validate users authorized to receive a software token. The software tokens contain:

- Personal Identity Verification (PIV) certificate
- Organizational affiliation
- Agency
- Department
- Expiration date
- Name
- DoD Electronic Data Interchange Person Identifier
- Date of birth
- Personnel category
- Pay category
- Benefits information
- Organizational affiliation
- Pay grade

Software tokens are stored in a secure location and access to this information is limited to authorized system administrators. These certificates are used to implement multifactor authentication mechanisms. The PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor.
Five Eyes (FVEY) is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are parties to the multilateral UKUSA Agreement, a treaty for cooperation in intelligence.

5.2 Describe any potential threats to privacy, such as insider threat, 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.)

The DOC ITSBP and NS3 Cybersecurity Program establishes policies, procedures, and requirements to protect classified and controlled unclassified information (CUI) that, if disclosed, could cause damage to national security. There is a possibility of insider threat which may occur, for example, a disgruntled employee has shared confidential information with media. All users are required to complete security awareness training on recognizing and reporting potential indicators of insider threat. Annual required training courses such as:

- DOC Controlled Unclassified Information (CUI) Basic User Awareness Training
- Cyber Security Awareness Training
- Derivative Classification
- Insider Threat Training
- How to Protect Personally Identifiable Information (PII) and Business Identifiable Information (BII)
- Marking Classified Information

| |
|---|
| Special Access Programs: A Special Access Program (SAP) is established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. Any user that requires SAP is required to take the annual Special Access Programs (SAP) training. |

## 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 | X | | |
| DOC bureaus | X | | |
| Federal agencies | X | | |
| State, local, tribal gov't agencies | | | |
| Public | | | |
| Private sector | | | |
| Foreign governments | | | X |
| Foreign entities | | | |
| Other (specify): | | | |

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

| | |
|---|---|
| | Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. |
| | No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. |
| X | No, the bureau/operating unit does not share PII/BII with external agencies/entities. |

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

| | |
|---|---|
| X | 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: Department of Defense Information Networks (DoDIN), technical controls include boundary protection mechanisms and network segmentation such as Firewalls, Routers, Switches, DLP and Encryption TACLANE. |
| | No, this IT system does not connect with or receive information from another IT system(s) authorized to |

| | |
|---|---|
| | process PII and/or BII. |

6.4 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 | X |
| Contractors | X | | |
| 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.)*

| | | |
|---|---|---|
| X | 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: _____. | |
| X | Yes, notice is provided by other means. | Specify how: When an individual completes the I-9 Instructions for Employment Eligibility Verification, they consent that the PII information collected may be disclosed. |
| | No, notice is not provided. | Specify why not: |

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

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to decline to provide PII/BII. | Specify how: Selected individuals for employment have the opportunity to decline to provide the requested information by not submitting the information, which will impede eligibility for the position they were selected for. The forms used are I-9 Instructions for Employment Eligibility Verification, which informs the individual that providing information is voluntary. Not providing the PII information may prevent completion of the investigation. |
| | No, individuals do not have an opportunity to decline to provide | Specify why not: |

| | | |
|---|---|---|
| | PII/BII. | |

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

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to consent to particular uses of their PII/BII. | Specify how: During the enrollment process for PIV individuals consent to particular uses of PII. When an individual completes the I-9 Instructions for Employment Eligibility Verification they consent that the PII information collected may be disclosed. |
| | 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.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to review/update PII/BII pertaining to them. | Specify how: Yes, the Individuals may contact the OHRM personnel or NS3 to review or update their personal information. Upon completion of the I-9 Instructions for Employment Eligibility Verification the individual has the opportunity to review and update prior to submission. Some investigations will include an interview with the individual. This provides the opportunity to update, clarify, and explain information that was provided from the individual. If there is no interview, then it is assumed that they will contact OHRM or NS3. |
| | 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.)*

| | |
|---|---|
| X | All users signed a confidentiality agreement or non-disclosure agreement. |
| X | All users are subject to a Code of Conduct that includes the requirement for confidentiality. |
| X | Staff (employees and contractors) received training on privacy and confidentiality policies and practices. |
| X | Access to the PII/BII is restricted to authorized personnel only. |
| | Access to the PII/BII is being monitored, tracked, or recorded.<br>Explanation: The NS3 audit and accountability controls have been implemented to record, monitor and detect unauthorized use of Network C. Event logs and policy violation logs are monitored routinely. Network C's implements system monitoring through a variety of continuous monitoring tools and techniques (e.g., malicious code protection software, scanning tools, and network monitoring software). Indicators of potential attacks and unauthorized access are monitored by the NS3 system administrators. |

| | |
|---|---|
| X | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): ___09/28/2021_____<br>☐ This is a new system. The A&A date will be provided when the A&A package is approved. |
| X | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |
| X | 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). |
| X | A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks. |
| X | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| | Contracts with customers establish DOC 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).*

NS3 uses best practice methods to protect PII for maximum security and regulatory compliance. The technology security measures used to protect PII/BII on System C include but not limited to the following:
1. Managed boundary protection mechanisms (Firewalls, Routers, Switches, and Encryption devices such as TACLANEs) isolate systems from outsiders and other DOC systems.
2. Least privilege access controls using group policy and Active Directory.
3. Automated mechanisms such as IBM BigFix to maintain an up-to-date, complete, accurate, and readily available asset inventory and baseline configuration of the information system.
4. Credentialed vulnerability scans executed weekly to identify vulnerabilities, system software and assess system weaknesses.
5. Intrusion Detection Systems and Intrusion Prevention Systems functions are installed at the firewall interfacing to the DODIN and internal system connections.
6. Data Loss Prevention software (SolarWinds) to ensure sensitive data is not lost, misused, or accessed by unauthorized users.

## Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X___ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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."

| | |
|---|---|
| X | Yes, this system is covered by an existing system of records notice (SORN).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br>Department 13 – Investigative and Security Records<br>Department 25 – Access Control and Identity Management System |
| | 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.)*

| | |
|---|---|
| X | There is an approved record control schedule.<br>Provide the name of the record control schedule: Retention and Disposal: Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). Unless retained for specific, ongoing security investigations, for maximum security facilities, records of access are maintained for five years and then destroyed. For other facilities, records are maintained for two years and then destroyed. All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22, approved by NARA. |
| | 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: |
| X | 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 | X | Overwriting | |
| Degaussing | X | Deleting | X |
| 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, and does not have to be 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. |
| X | 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 level. *(Check all that apply.)*

| | | |
|---|---|---|
| X | Identifiability | Provide explanation:<br>SSN not stored. |
| X | Quantity of PII | Provide explanation:<br>There are a limited number of authorized users |
| X | Data Field Sensitivity | Provide explanation:<br>PII data field contains sensitive PII data. |
| | Context of Use | Provide explanation: |
| X | Obligation to Protect Confidentiality | Provide explanation:<br>CNSS, OMB, NIST and DOC requires protection of PII. |
| X | Access to and Location of PII | Provide explanation:<br>Access to PII is restricted to authorized personnel. |
| | 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.)

| |
|---|
| NS3 limits the amount of PII collected from its sources. NS3 only collects PII directly from the individual or authorized Trusted Agents (TAs).<br><br>The TAs are mainly used with new account and Public Key Infrastructure Token request from our field offices. The TAs validates the individual's identity and credentials, transmits the information to NS3. The information is then reverified by the Registration Authority for authorized input into the system.<br><br>The internal PII information collected is transferred hand to hand from the individual(s) to the authorized collector and/or transferred via Kite Works (encrypted email). All transmitted information requires two-factor authentication and use of a Personal Identity Verification card for integrity and non-repudiation. NS3 collects the least amount of PII for account establishment and PKI assurance. All data is properly disposed at the end of its life cycle. |

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.<br>Explanation: |
| X | 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.

| | |
|---|---|
| X | Yes, the conduct of this PIA results in required technology changes.<br>Explanation:<br>Additional privacy controls were required, including encryption and data minimization security controls. |
| | No, the conduct of this PIA does not result in any required technology changes. |