Template Version Number: 01-2021

# U.S. Department of Commerce
# U.S. Census Bureau

## Privacy Impact Assessment
## for the
## Office of the Chief Information Officer (OCIO)
## Telecommunications Office (TCO) Data Communications

Reviewed by: Donna Neal (acting), 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

Donna Neal

Digitally signed by Donna Neal
Date: 2023.09.20 15:57:47 -04'00'

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

# U.S. Department of Commerce Privacy Impact Assessment
# U.S. Census Bureau/Office of the Chief Information Officer (OCIO)
# Telecommunications Office (TCO) Data Communications

**Unique Project Identifier: 006-000401400**

**Introduction: System Description**

*Provide a brief description of the information system.*

| *The response must be written in plain language and be as comprehensive as necessary to describe the system.* |
|---|
| The OCIO Data Communications System is the foundational Information Technology (IT) system that sustains the day-to-day business activities to provision government services within the Census Bureau. This IT system covers the Census Bureau telecommunications infrastructure. |

Address the following elements:

*(a) Whether it is a general support system, major application, or other type of system*

General Support System

*(b) System location*

- U.S., Census Bureau, Suitland, MD
- U.S., Census Bureau, Bowie, MD
- AWS GovCloud, AWS Region US-East, VA
- Microsoft Azure Commercial (O365), Azure Region East US, VA
- National Processing Center (NPC), Jeffersonville, IN

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

The OCIO Data Communications system is a core system at the Census Bureau that provides secured access to services such as internet, e-mail services, file access, printing services and other information system services and interconnects with all of the IT systems at the Census Bureau. OCIO Data Communications receives Personally Identifiable Information (PII) from a OCIO Human Resources Application named CAMPIN and OCIO Commerce Business Systems, in a one-way pull, for the creation of new employee accounts.

The NPC Call Center video screen captures, and audio recordings are stored on servers within the OCIO Network Services System and accessed only by authorized individuals (i.e., call center supervisors and call center managers) for the purpose of quality assurance and call center employee training.

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

OCIO Data Communications General Support System serves as the transport system utilized by data collection/dissemination systems and is therefore not a data collection/dissemination system itself. As the medium to interconnect the various information systems deployed in the Census Bureau, OCIO Data Communications utilizes PII for the purpose of administrative matters. These information systems provide services such as authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, mobile devices, and voice and video teleconferencing services. The PII maintained by the IT system consists of federal employee, contractor, and external user account information required to access Census Bureau resources (e.g., user ID, name, and email address).

The OCIO Data Communications Systems contain a Microsoft O365 application, the digitized "Likeness and Profile Release" form, that will be used to establish the identity of an individual and capture the consent from the public, regarding photographs taken at Census Bureau events.

At Census Bureau events, photographs of event attendees may be captured but will only be used if the individual identifies themselves and provides consent. If the event goer chooses to consent to their photograph being used by the U.S. Census Bureau, they will be handed a Census Bureau device with a copy of the digitized Likeness and Release form open and required to input their name and confirm that they are over the age of 18. Once they input their name and confirm they are over 18, the app will require them to take a selfie for purposes of identifying the signer, followed by the provision of a signature; an image capture of their signature will be saved for consent purposes. If the individual is under the age of 18, the app will require parental name, email address consent and signature. This information will be securely exported to the OCIO Enterprise Applications. Each individual's consent form will be assigned a unique identifier and will not be searchable by PII.

Another purpose of OCIO Data Communications Systems is for quality assurance and call-center employee training via the Associate Director for Field Operations (ADFO) National Processing Center (NPC) Call Center Monitoring; The Call Center monitoring is a client application that is installed on NPC Call Center Employees' Computers and when it detects an incoming call, it starts to capture the employee's computer screen and call audio; this could include assisting an individual in completing a survey. This is intended to support quality assurance as well as to document incidents warranting dismissal. This data can be used by the Census Bureau for

personnel enforcement. An assortment of PII may be captured via the video screen recordings and audio recordings depending on the nature of the call as members of the public opt to complete surveys via the call center. Although Title 13 information may be incidentally captured in the screen capture recordings and audio recordings, the purpose is not for Title 13 survey processing, but solely for quality assurance and call-center employee training. Incidental Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. No PII/BII captured via the screen capture recordings is searchable by personal identifier.

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

Information in is retrieved by the specific network device or application console by Census Bureau Telecommunications Office (TCO) administrators. For the digitized Likeness and Release form, information is retrieved upon by date and/or unique identifier. No PII/BII captured is searchable by personal identifier.

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

Information in the OCIO Data Communications system varies based on the technology. All data is securely communicated through Secure Message Transfer Protocol (SMTP), Transport Layer Security (TLS) 1.2, and Secure Shell (SSH).

*(g) Any information sharing*

The OCIO Data Communications systems share information (authentication checks) with Census Bureau IT systems, but sensitive PII/BII is not shared. The 0365 app and data that captures consent will reside here, however a subset of the captured data will be exported and stored alongside the actual assets (photos and videos captured at events) in the OCIO Enterprise Applications Systems. Call Center video screen captures, and audio recordings will be stored on servers within the Census Bureau's OCIO Network Services systems and accessed only by authorized individuals (call center supervisors and call center managers) for the purpose of quality assurance and call center employee training.

In support of the Continuous Diagnostic Monitoring (CDM) initiative, OCIO Data Comunications sends data to NIST. The data contained is Census User account data such as name, email, job title, manager, etc. and is requested by the Department Of Commerce (DOC) in support of DOC CDM initiatives.

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

5 U.S.C 301 and 44 U.S.C 3101

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

Moderate

## 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.

___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.

## 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 | x[1] | | | | |
| n. Other identifying numbers (specify): | | | | | |
| *Explanation for the business need to collect, maintain, or disseminate the Social Security number, including | | | | | |

[1] *Data captured in this system may include Title 13 survey respondent information and information from Census employees. Title 13 survey respondent information may be incidentally captured via screen capture recording/audio recording by the NPC call center not for Title 13 purposes but instead for quality assurance and call center employee training. Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. No T13 PII/BII captured via the screen capture recordings/audio recording is searchable by personal identifiers.*

| truncated form: N/A |
|---|

| **General Personal Data (GPD)** | | | | | |
|---|---|---|---|---|---|
| a. Name | x* | h. Date of Birth | x* | o. Financial Information | |
| b. Maiden Name | x* | i. Place of Birth | x* | p. Medical Information | |
| c. Alias | | j. Home Address | x* | q. Military Service | |
| d. Gender | x* | k. Telephone Number | x | r. Criminal Record | |
| e. Age | x* | l. Email Address | x | s. Marital Status | |
| f. Race/Ethnicity | x* | m. Education | x* | t. Mother's Maiden Name | x* |
| g. Citizenship | | n. Religion | | | |
| u. Other general personal data (specify): | | | | | |
| * Title 13 data may be incidentally captured via screen capture recording/audio recording by the NPC call center not for Title 13 purposes but instead for quality assurance and call center employee training. Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. No T13 PII/BII captured via the screen capture recordings/audio recording is searchable by personal identifiers. | | | | | |

| **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): | | | | | |
| * Title 13 data may be incidentally captured via screen capture recording/audio recording by the NPC call center not for Title 13 purposes but instead for quality assurance and call center employee training. Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. No T13 PII/BII captured via the screen capture recordings/audio recording is searchable by personal identifiers. | | | | | |

| **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 | x | h. Eye Color | | m. DNA Sample or Profile | |
| d. Video Recording | x | i. Height | | n. Retina/Iris Scans | |
| e. Photographs | x | j. Weight | | o. Dental Profile | |
| p. Other distinguishing features/biometrics (specify): Image Capture of Signatures | | | | | |

| **System Administration/Audit Data (SAAD)** | | | | | |
|---|---|---|---|---|---|
| a. User ID | x | c. Date/Time of Access | x | e. ID Files Accessed | |
| b. IP Address | x | f. 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 | x | Email | | | |
| Other (specify): | | | | | |

| **Government Sources** | | | | | |
|---|---|---|---|---|---|
| Within the Bureau | x | 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.

Census Bureau Information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any IT system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention (DLP) solution as well.

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): | | | |

| | |
|---|---|
| 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 | X | Building entry readers | |
| Video surveillance | | Electronic purchase transactions | |
| Other (specify): Video Screen Capture Recording and image capture of signatures. | | | |

| | |
|---|---|
| | 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 | | 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): Quality assurance and call center training; For Identity and Consensual Purposes | | | |

## 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).

The OCIO Data Communications system serves as the medium to interconnect the various Census Bureau information systems that are deployed in addition to providing services such as authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, and voice and video teleconferencing services. For these functions listed, the PII collected is account information such as user ID, name, telephone and email address and is from federal employees and contractors who use internal email systems and the general public who sign up to external web sites. The information used is to allow users the ability to authenticate to Census Bureau systems.

The 0365 application will collect PII (name, selfie, and digital signature) from event participants (likely members of the public) for the purpose of identification and consent. The purpose of this tool is to identify and get consent from individuals whose photographs are taken by the U.S. Census Bureau. If consent is granted, the photos can be used for promotional purposes; if not the photo will not be used.

In regard to Call Center Monitoring functionalities used to support quality assurance and call center training; an assortment of PII may be captured via the employee screen recording and audio recordings. Title 13 PII may be incidentally collected from the public if they opt to complete their survey via the call center.

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 U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data. Incidental Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The potential disclosure of sensitive personal PII through email is mitigated by the use of the Data Loss Prevention (DLP) tool which can quarantine possible sensitive PII from being sent. Additionally, employees and contractors undergo mandatory annual Data Stewardship training that includes the appropriate method of sending sensitive information via an approved encryption tool.

## 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 | | X |
| DOC bureaus | X | X | |
| 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 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:<br><br>OCIO Data Communications interconnects with all of the Census Bureau IT systems.<br><br>OCIO Data Communications receives PII from the OCIO Human Resources Application named CAMPIN and OCIO Commerce Business Systems, in a one-way pull, for the creation of new employee accounts.<br><br>OCIO Data Communications shares information (authentication checks) with Census Bureau IT systems, but sensitive PII/BII is not shared.<br><br>The 0365 app and data that captures consent will reside here however a subset of the captured data will be exported and stored alongside the actual assets (photos and videos captured at events) in OCIO Enterprise Applications Systems.<br><br>Call Center video screen captures and audio recordings will be stored on servers within the Census Bureau OCIO Network Services Systems and accessed only by authorized individuals (call center supervisors and call center managers) for the purpose of quality assurance and call center employee training.<br><br>The OCIO Data Communications IT system uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well. |
| | 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.)*

| | | |
|---|---|---|
| | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. | |
| X | 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: https://www.census.gov/about/policies/privacy.html<br>Title 13 Survey respondents calling into the call center were provided a Privacy Act Statement either through an introductory letter or as a part of the questionnaire. These respondents are also given the opportunity to opt in or out of the audio recordings/video screen capture when calling into the call center. | |
| X | Yes, notice is provided by other means. | Specify how: For the digitized Likeness and Release form, a privacy notice is displayed before the user provides consent. Event participants must accept the full legal text of the release form prior to data entry. The text details what constitutes their "Profile" and waives all usage rights. |
| X | No, notice is not provided. | Specify why not: For all other OCIO Data Communications Systems (authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, mobile devices, and voice and video teleconferencing services), employees & contractors must consent to the uses of their PII to work at the Census Bureau. If a user chooses not to consent, they will not be employed at the Census Bureau. |

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: For Call Center Monitoring, the callers are notified of screen capture recording and audio recording and have the option to decline both, which will allow the employee to disable the recordings.<br><br>In regard to the digitized Likeness and Release form, users have the ability to decline to provide their data/PII. This means that their photograph or the likeness of, from recent events will not be used by the Census Bureau. For minors, under the age of 18, parental consent is required. |
| X | No, individuals do not have an opportunity to decline to provide PII/BII. | Specify why not: For all other OCIO Data Communications System applications (authentication for internal and external customers, network security, LAN/WAN, e-mail, Internet access, remote access, mobile devices, and voice and video teleconferencing services), employees & contractors must consent to the uses of their PII to work at the US Census Bureau. If a user chooses to decline to provide their PII, they will not be employed at the Census Bureau. |

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: For Call Center Monitoring, the callers are notified of the use of the screen capture and audio recordings (quality assurance and Call Center employee training) and have the option to decline, which will allow the employee to disable the recordings.<br><br>For the digitized Likeness and Release form, users have the opportunity to consent by choosing to sign the form or declining to sign the consent form. If users do not consent to the uses of their PII, and decline to sign the form, this means that their photograph or the likeness of, from recent events will not be used by the Census Bureau. For minors, under the age of 18, parental consent is required. |
| X | No, individuals do not have an opportunity to consent to particular uses of their PII/BII. | Specify why not: For all other OCIO Data Communications Systems applications (except audio and screen capture tool) employees & contractors must consent to the uses of their PII to work at the Census Bureau. If a user chooses not to consent, they will not be employed at the Census Bureau. External users must agree to the acceptable use prior to being able to authenticate to various information systems. |

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: For most OCIO Data Communications Systems employees and contractors may review/update PII via the applicable OCIO human resources applications (OCIO CBS and CAMPIN). |
| X | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: For Call Center Monitoring, only the call center employee's screen is captured. PII/BII cannot be updated via a screen capture.<br><br>For the digitized Likeness and Release form, users will not have the ability to review/update their PII/BII. |

## 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. |
| X | Access to the PII/BII is being monitored, tracked, or recorded.<br>Explanation: Only authorized government/contractor personnel are allowed to access PII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J |

| | |
|---|---|
| | Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records. |
| 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): _____7/18/2023_____<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).*

Census Bureau Information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any IT system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a (Data Loss Prevention (DLP) solution as well.

## **Section 9**: Privacy Act

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

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

__X__ 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."

| | |
|---|---|
| | 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)*: |
| | Yes, a SORN has been submitted to the Department for approval on (date). |
| X | 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:<br><br>• **GRS 2**<br>• **GRS 3.1**<br>• **GRS 3.2**<br>• **GRS 4.2**<br>• **GRS18 – Section#22**<br><br>In regard to the call center monitoring application, incidental Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. |
| | 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 | | Overwriting | X |
| Degaussing | X | Deleting | X |
| Other (specify): Incidental Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days. | | | |

## 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. |
| X | 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 level. *(Check all that apply.)*

| | | |
|---|---|---|
| X | Identifiability | Provide explanation: PII collected can be indirectly used to identify individuals or if combined with other data elements may uniquely identify an individual. |
| X | Quantity of PII | Provide explanation: 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. |
| X | Data Field Sensitivity | Provide explanation: Data fields, alone or in combination, have little relevance outside the context. |
| X | Context of Use | Provide explanation: The personally identifiable information (PII) housed maintained by the IT system is account information (such as user ID, name, and email address) for federal employees, contractors, and external users in order to access Census Bureau resources. |
| X | Obligation to Protect Confidentiality | Provide explanation: PII maintained is required to be protected. |
| X | Access to and Location of PII | Provide explanation: The PII is located on computers (including laptops) and on a network, and IT systems controlled by the Census Bureau. Access is limited to those with a need-to-know including the Census Bureau regional offices and survey program offices, etc. Access is allowed by Census Bureau-owned equipment outside of the physical locations owned by the Census Bureau only with a secure connection. Backups are stored at Census Bureau-owned facilities.<br><br>PII is also located on U.S. Census Bureau authorized vendor systems. Access is limited to those with a need-to-know for authorized U.S. Census Bureau contractors and employees. |
| | 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.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data. Title 13 screen capture recordings are deleted after 90 days and audio recordings are deleted after 180 days.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution.

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.

| | |
|---|---|
| | Yes, the conduct of this PIA results in required technology changes.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required technology changes. |