

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



Privacy Impact Assessment
for
CEN15 Centurion

Reviewed by: Byron Crenshaw, 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

Lisa Martin

for Dr. Jennifer Goode

05/26/2021

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

Date

**U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/ CEN15 Centurion**

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

CEN15 Centurion is a major application

(b) System location

CEN15 is located at the Bowie Computer Center.

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

CEN15 interconnects with internal Census Bureau IT systems to leverage enterprise services (CEN01 Data Communications, CEN16 Network Services) and inherit security controls provided by the Enterprise Common Control Providers (ECCP). CEN15 also interconnects with the following internal Census Bureau systems: CEN03 Economic Census and Surveys and Special Processing, CEN05 Field, CEN07 Geography, CEN18 Enterprise Applications, CEN30 American Community Survey, and CEN36 Associate Director for Economic Programs (ADEP) Innovation Technology Office (ITO). In addition, CEN15 connects with an external system at the Bureau of Industry and Security.

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

CEN15 Centurion is a web-based application used for the design, delivery, and execution of surveys, censuses, and other data collection and data exchange efforts over the Internet. Centurion allows the Census Bureau to collect data more cost effectively and with a higher degree of accuracy as compared to equivalent traditional data collection methods.

Information collected via the Centurion IT system includes data covered by Title 13 and Title 26 collection authorities for demographic and economic surveys. Standard web browser clients are used to access the Centurion IT system. Members of the public accessing Centurion are survey or census respondents. Information collected via Centurion includes, but is not limited to, names, telephone numbers, email addresses, etc.

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

Information in CEN15 Centurion is retrievable by a personal identifier such as name, by authorized Centurion administrators.

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

Information collected from survey respondents is provided back to the survey sponsors through Secure File Transfer Protocol (SFTP). Users submit survey information via applications using secure protocols such as HTTPS.

(g) Any information sharing conducted by the system

The Centurion application allow survey sponsors, both internally (program area sponsors) and externally (sponsors of reimbursable surveys), access to their specific data. In other words, the data is shared by allowing Census Bureau personnel and data sponsors access to the data. Census Bureau personnel may have to process some data for external survey sponsors. The Centurion system automatically generates output files for each survey in one of many supported output formats. Output files are generated on a predetermined schedule and delivered to the internal Bureau survey areas can then pick up their files or are delivered directly to where internal Bureau survey areas servers using the secure protocol.

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

13 U.S.C. Sections 8(b), 131, 161, 141, 182, 193 and 26 U.S.C 6103(j).

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

The FIPS 199 security impact category for CEN15 is 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 (version 01-2015 or 01-2017).
- _____ 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 | X | g. Passport | | k. Financial Transaction | |
| c. Employer ID | X | h. Alien Registration | | l. Vehicle Identifier | X |
| d. Employee ID | | i. Credit Card | | m. Medical Record | |
| e. File/Case ID | X | | | | |
| 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 | X |
| b. Maiden Name | X | i. Place of Birth | X | p. Medical Information | X |
| c. Alias | X | j. Home Address | X | q. Military Service | X |
| d. Gender | X | k. Telephone Number | X | r. Criminal Record | |
| e. Age | X | l. Email Address | X | s. Physical Characteristics | X |
| f. Race/Ethnicity | X | m. Education | X | t. Mother's Maiden Name | |
| g. Citizenship | X | 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 | X | j. Proprietary or Business Information | |
| c. Work Address | X | g. Work History | X | k. Procurement/contracting records | |

| | | | | | |
|---------------------------------------|---|--|--|--|--|
| d. Work Telephone Number | X | h. Employment Performance Ratings or other Performance Information | | | |
| i. 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 | X | n. Retina/Iris Scans | |
| e. Photographs | | j. Weight | X | 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 | |
| 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 | X |
| 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.

Survey areas mail invitations to potential survey respondents that include credentials that the respondent must use to login and provide their information, thus providing us reasonable assurance of the correct respondent. Likewise, Centurion contains an extensive amount of real-time edits to validate that the information that is being reported by the respondents is accurate to the best of ability.

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. |
| 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 | | 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 | | To promote information sharing initiatives | |
| For litigation | | For criminal law enforcement activities | |
| For civil enforcement activities | | For intelligence activities | |
| To improve Federal services online | X | For employee or customer satisfaction | |
| For web measurement and customization technologies (single-session) | | For web measurement and customization technologies (multi-session) | |
| Other (specify): For statistical purposes (i.e., Censuses/Surveys) | | | |

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).

Centurion collects PII and BII from members of the public for several censuses and surveys conducted by the Census Bureau.

To improve Federal services online: Customers are able to submit surveys via Centurion.

For statistical purposes (i.e., Censuses/Surveys): The Economic Census is the U.S. Government's official five-year measure of American business and the economy conducted by the U.S. Census Bureau. Responding to the Census is required by law. Forms are mailed to approximately 4 million businesses, including large, medium, and small companies representing all U.S. industries. Respondents are asked to provide a range of operational and performance data for their companies.

Centurion also collects data for the American Community Survey (ACS). This ongoing survey provides data annually, giving communities the current information they need to plan investments and services. Information from the survey generates data that help determine how more than \$400 billion in federal and state funds are distributed each year.

Centurion also collects data for the Decennial Census tests, demographic, and other economic survey collections. The collections are for statistical purposes such as the Annual Wholesale Trade Survey (AWTS), Private School Survey (PSS), Annual Retail Trade Report Survey (ARTS), Annual Survey of Local Government Finances (ALFIN), etc.

- 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.

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.

The information in the CEN15 is handled, retained and disposed of in accordance with appropriate federal record schedules.

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 | | |
| 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 | <p>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:</p> <p>CEN15 interconnects with Census Bureau systems CEN03: Economic Census and Surveys and Special Processing, CEN05 Field, CEN07 Geography, CEN18 Enterprise Applications, CEN30 American Community Survey, and CEN36: Associate Director for Economic Programs (ADEP) Innovation Technology Office (ITO).</p> <p>CEN15 Centurion also interconnects with the Bureau of Industry and Security (BIS). Centurion creates extracts of data and pushes them to BIS; BIS does not have access to Centurion via this interconnection.</p> <p>The CEN15 Centurion 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 Bureau facilities that house Information Technology systems. Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.</p> |
| | 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 ¹ | X | 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. | |
| 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: http://www.census.gov/about/policies/privacy/privacy-policy.html | |
| X | Yes, notice is provided by other means. | Specify how: via Privacy Act Statements provided to respondents prior to responding to a census or survey. Centurion has a link at the bottom of every survey that directs the respondent to the Census Bureau Privacy Policy. |
| | 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: Various surveys maintained by the CEN15 IT system are voluntary and therefore not required to provide PII/BII. |
| X | No, individuals do not have an opportunity to decline to provide PII/BII. | Specify why not: Some surveys and the Economic Census are mandatory as required by 13 U.S.C. Individuals are informed of this by one of the following: via Privacy Act Statements upon login, letter, interview, or during data collection. |

- 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: Various surveys maintained by the CEN15 IT system are voluntary and therefore not required to provide PII/BII. |
| X | No, individuals do not have an opportunity to consent to particular uses of their PII/BII. | Specify why not: Some surveys and the Economic Census data maintained by the CEN15 IT system are mandatory as required by 13 U.S.C. The data are used for statistical and |

¹ The survey respondent has access to their information only.

| | | |
|--|--|---|
| | | administrative purposes only and are exempt from consent to particular uses of PII/BII. |
|--|--|---|

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 the Economic Census and surveys maintained by the CEN015 IT system, individuals have the opportunity to provide updates to PII/BII data on the submitted survey or on the survey website. |
| X | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: For surveys that collect information for statistical purposes, respondents are exempt from review/update of PII/BII unless the Census Bureau contacts them to update the information. |

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. Explanation: Only authorized government/contractor personnel are allowed to access PII/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition 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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 07/08/2020 <input type="checkbox"/> 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 (POAM). |
| 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 ownership rights over data including PII/BII. |
| | Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers. |

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 BII/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 system within the Census 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 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)?

 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 | <p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i></p> <p>COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html</p> <p>COMMERCE/CENSUS-4, Economic Survey Collection- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html</p> <p>COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html</p> <p>COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-7.html</p> |
|---|--|

| | |
|--------------------------|--|
| <input type="checkbox"/> | Yes, a SORN has been submitted to the Department for approval on (date). |
| <input type="checkbox"/> | 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 | <p>There is an approved record control schedule. Provide the name of the record control schedule: DAA-0029-2015-0001</p> <p>N1-029-10-2, N1-029-10-3, N1-029-12-004, N1-029-10-4</p> <p>Company Statistics Division N1-29-10-1</p> <p>Economic Surveys Division N1-29-03-1NC1-29-80-15, NC1-29-79-4, NC1-29-78-15 NC1-29-78-8</p> <p>Manufacturing and Construction Division NC1-29-81-10</p> <p>Demographic Surveys: N1-29-99-5, N1-29-89-3, N1-29-87-3, N1-29-86-3, NC1-29-85-1, NC1-29-79-</p> |
| <input type="checkbox"/> | <p>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:</p> |
| X | Yes, retention is monitored for compliance to the schedule. |
| <input type="checkbox"/> | 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 | <input type="checkbox"/> | Overwriting | <input type="checkbox"/> |
| Degaussing | <input type="checkbox"/> | 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: PII collected can directly identify individuals |
| X | Quantity of PII | Provide explanation: The collection is for Census Bureau Censuses and surveys, therefore, a severe or catastrophic number of individuals would be affected if there was loss, theft or compromise of the data. |
| X | Data Field Sensitivity | Provide explanation: The PII, 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. |
| X | Context of Use | Provide explanation: PII/BII is collected by Centurion for statistical purposes and to improve federal services online. |
| X | Obligation to Protect Confidentiality | Provide explanation: PII/BII collected is required to be protected in accordance with 13 U.S.C. section 9. |
| X | Access to and Location of PII | Provide explanation: PII/BII is located on computers and other devices on a network controlled by the Census Bureau. Access limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals (e.g., of sponsoring agencies). Access only allowed by organization-owned equipment outside of the physical locations owned by the organization only with a secured connection. |
| | 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.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

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

Points of Contact and Signatures

| | |
|--|---|
| <p>System Owner Name: David J. Peters Office: Application Development & Services Division Phone: (301) 763-9359 Email: david.j.peters@census.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>DAVID</u> Digitally signed by DAVID PETERS Date signed: <u>PETERS</u> Date: 2021.01.25 08:43:27 -05'00'</p> | <p>Chief Information Security Officer Name: Beau Houser Office: Office of Information Security Phone: (301) 763-1235 Email: beau.houser@census.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.</p> <p>Signature: <u>BEAU</u> Digitally signed by BEAU HOUSER Date signed: <u>HOUSER</u> Date: 2021.02.02 09:04:26 -05'00'</p> |
| <p>Census Bureau Chief Information Officer Name: Gregg D. Bailey Office: Associate Director of IT & CIO Phone: (301) 763-0989 Email: Gregg.d.bailey@census.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>GREGG</u> Digitally signed by GREGG BAILEY Date signed: <u>BAILEY</u> Date: 2021.02.04 12:18:18 -05'00'</p> | <p>Business Authorizing Official Name: Office: N/A Phone: Email:</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>N/A</u> Date signed: _____</p> |
| <p>Census Bureau Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763-7997 Email: byron.crenshaw@census.gov</p> <p>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.</p> <p>Signature: <u>BYRON</u> Digitally signed by BYRON CRENSHAW Date signed: <u>CRENSHAW</u> Date: 2021.02.22 11:50:44 -05'00'</p> | <p>Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office (PCO) Phone: (301) 763-7997 Email: byron.crenshaw@census.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p>Signature: <u>BYRON</u> Digitally signed by BYRON CRENSHAW Date signed: <u>CRENSHAW</u> Date: 2021.02.22 11:51:14 -05'00'</p> |

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.