

# U.S. Department of Commerce

## U.S. Census



### Privacy Impact Assessment for the CEN01 Data Communications

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

**CATRINA PURVIS** Digitally signed by CATRINA PURVIS  
Date: 2020.09.21 19:14:34 -04'00'

04/14/2020

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

Date

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

**Unique Project Identifier: [Number]**

**Introduction: System Description**

CEN01 is the fundamental information IT system that sustains the day-to-day business activities to provision government services within the Census Bureau.

*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. Please answer each question (a) through (i) separately.*

*(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

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

CEN 01 serves as the medium of interconnection for client information systems within the Census Bureau network infrastructure wirelessly. This information system provides secured wireless access to services such as e-mail services, file access, printing services, and other information system services. A general transaction consists of account user verification for system access.

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

In section 4, it is identified that Data Communications GSS (CEN01) is collecting, maintaining, and/or disseminating PII for the purpose of administrative matters. CEN01 serves as the medium to interconnect the various Census Bureau information systems that are deployed. 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 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.

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

Information in CEN01 is mostly retrieved by the specific network device or application console by Census Bureau Telecommunications Office (TCO) administrators.

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

Information in CEN01 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 conducted by the system*

CEN01 shares information (authentication checks) with other systems, but sensitive PII/BII is not shared.

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

The legal authorities for data collections on this IT system are:  
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.)*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>				
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.

## **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.)*

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

<b>General Personal Data (GPD)</b>				
a. Name	x	g. Date of Birth		m. Religion
b. Maiden Name		h. Place of Birth		n. Financial Information
c. Alias		i. Home Address		o. Medical Information
d. Gender		j. Telephone Number	x	p. Military Service
e. Age		k. Email Address	x	q. Physical Characteristics
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name
s. Other general personal data (specify): The items are collected from the general public who sign up to external web sites. Email addresses are from work.				

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

<b>Distinguishing Features/Biometrics (DFB)</b>				
a. Fingerprints		d. Photographs		g. DNA Profiles
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans
c. Voice		f. Vascular Scan		i. Dental Profile

Recording/Signatures				
j. Other distinguishing features/biometrics (specify):				

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

<b>Other Information (specify)</b>

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

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

<b>Government Sources</b>				
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies
State, Local, Tribal		Foreign		
Other (specify):				

<b>Non-government Sources</b>				
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. 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 conferencing			

	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.)

<b>Purpose</b>			
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):			

### **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 Data Communications (CEN01) IT 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 . The PII collected is account information such as userID, 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.

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

The potential disclosure of sensitive personal PII through email is mitigated by the use of the 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 (such as Kiteworks).

**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			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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

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

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>Lightweight Directory Access Protocol (LDAP) is connected to CAMPIN and CBS systems, in a one-way pull, for the creation of new employee accounts.</p>
---	---

	The CEN01 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.

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

<b>Class of Users</b>			
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.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
	Yes, notice is provided by other means.	Specify how: Notice that PII is collected, maintained, or disseminated in the IT system is provided by the login banner to the network.
x	No, notice is not provided.	Specify why not:

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
x	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Users (employees & contractors) must consent to the uses of their PII to work at the US 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.

- 7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of

their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
x	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Users must consent to the uses of their PII to work at the US 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: Individuals may review/update PII via the applicable human resources applications. External users must agree to the acceptable use prior to being able to authenticate to various information systems.
	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.
x	Access to the PII/BII is being monitored, tracked, or recorded. 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 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): <u>7/20/2018</u> <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 (POA&M).
x	A security assessment report has been reviewed for the supporting 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.
	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).*

<p>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:</p> <p>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</p> <p>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.</p>
--

## **Section 9: Privacy Act**

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

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

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
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. Provide the name of the record control schedule:
---	---

	<b>GRS 2</b> <b>GRS 3.1</b> <b>GRS 3.2</b> <b>GRS 4.2</b> <b>GRS18 – Section#22</b>
	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:
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.)*

<b>Disposal</b>			
Shredding		Overwriting	x
Degaussing		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 as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

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

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 collected is required to be protected in accordance with: 5 U.S.C and 44 U.S.C 3101
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.  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.)

Employees and contractors undergo mandatory annual Data Stewardship training that includes the appropriate method of sending sensitive information via an approved encryption tool (such as Kiteworks).

- 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.