

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



**Privacy Impact Assessment  
for the  
CEN17 Client Services**

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: 2020.08.12 09:54:28 -04'00' 08/12/2020

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

Date

**U.S. Department of Commerce Privacy Impact Assessment  
U.S. Census Bureau/ CEN17 Client Services**

**Unique Project Identifier: 006-000401700**

**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*

CEN17 Client Services is general support system

*(b) System location*

CEN17 Client Services is located at Bowie Computing Center.

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

CEN17 Services interconnects with other systems. The components of the CEN17 Client Services security plan share security tokens internally with CEN01 Data Communications and the CEN16 Network Services security plan components. For example, a CEN17 component may request authentication of username, PIV, and Personal Identification Number (PIN) from CEN01 component. The CEN17 component may then forward information of the authenticated security token along with a request to access the data stored by that username on the CEN16 component. CEN17 also connects with CEN04 to receive inventory control, account management, personnel management and PII data from CEN04 CBS database. CEN17 also connects with CEN21 to automate the exit process after an employee is terminated.

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

The purpose of the IT system is for administrative purposes. i.e., to assist in the management and maintenance of IT resources, and for providing help desk assistance and end user services.

A typical transaction on the components of CEN 17 Client Services would be login and authentication to a desktop or virtual desktop using applications such as email, Microsoft Office products, web browsers, and databases. The authentication of customers to gain access

to an IT system is processed externally to CEN 17 (by connection to CEN01 Data Communications).

In order for employees to use the desktops or virtual desktops, they must have a user ID, completed the data stewardship training, and have received special sworn status (this status acknowledges that the individual has been sworn to protect information collected by the Census Bureau for life). In addition, a Personal Identity Verification (PIV) card is required. Secure ID is required for external access. PIV card is required for internal access.

The component used for managing cases is a tool that allows specially trained call center staff to capture the initial documentation of the issue. The issue is input, routed, and stored in the case management portion of the system that is carefully segregated from all other records. Only those with a need-to-know may access or view records.

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

In order for employees to use the desktops or virtual desktops, they must have a user ID, completed the data stewardship training, and have received special sworn status (this status acknowledges that the individual has been sworn to protect information collected by the Census Bureau for life). In addition, a Personal Identity Verification (PIV) card is required. Secure ID is required for external access. PIV card is required for internal access.

The component used for managing cases is a tool that allows specially trained call center staff to capture the initial documentation of the issue. The issue is input, routed, and stored in the case management portion of the IT system that is carefully segregated from all other records. Only those with a need-to-know may access or view records.

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

The components of the CEN17 Client Services security plan share security tokens internally with the CEN01 Data Communications and the CEN16 Network Services security plan components. For example, a CEN 17 component may request authentication of username, PIV, and Personal Identification Number (PIN) from a CEN01 component. The CEN17 component may then forward information of the authenticated element to a component within CEN16, such as providing an authenticated security token along with a request to access the data stored by that username on the CEN16 component. CEN17 shares information about the addition and retirement of hosts with CEN16 Gov CloudForms. This allows automatic updates of the assets. This information is transmitted using HTTPS. CEN17 has an interconnection agreement with CEN21 Census Hiring and Employment

Check system. This interconnection automates the exit process after a Census Bureau employee terminates employment. Data is transmitted via HTTPS.

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

The components of the CEN17 Client Services security plan share security tokens internally with the CEN01 Data Communications and the CEN16 Network Services security plan components. For example, a CEN17 component may request authentication of username, PIV, and Personal Identification Number (PIN) from a CEN01 component. The CEN17 component may then forward information of the authenticated element to a component within CEN16, such as providing an authenticated security token along with a request to access the data stored by that username on the CEN16 component. CEN17 shares James Bond ID information with CEN21 Census Hiring and Employment Check system to facilitate the automation of employee termination process.

CEN17 may also share information from the sub-component that manages cases, on a case-by-case basis, within the Census Bureau, with other DOC bureaus, federal agencies, and state, local, and tribal government agencies. This includes the Commerce Incident Response Team, law enforcement, and the FBI.

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

5 U.S.C. 301; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 44 U.S.C. 3301; Homeland Security Presidential Directive 12

*(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.
- \_\_\_\_\_ 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).
- 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 01-2017 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.)

<b>Identifying Numbers (IN)</b>					
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	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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

<b>Work-Related Data (WRD)</b>					
a. Occupation		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			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

--

<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 Recording/Signatures		f. Vascular Scan		i. Dental Profile	
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	X
b. IP Address	X	d. Queries Run	X	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	X	Hard Copy: Mail/Fax		Online	X
Telephone	X	Email			
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.

Information entered into the information system is verified during completion of the Remedy entrance ticket created for each user that is on-boarded. The user must provide verification of the information provided before the ticket is closed.

#### 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.)

<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).

Information about federal employees and contractors, such as name, user ID, occupation, employee number, business associates, PIV number, date and time of access, and active/separated status is used to assist in the management and maintenance of IT resources within the CEN 17 Client Services security plan.

In addition, the IT service case management system also shares and stores some of the same information for the purpose of providing help desk assistance and end user services. This information is used to generate audit reports on system patch levels, last local/network login of user accounts, malware infections, current system software inventory, etc. The information is not collected for any purpose other than authentication and management of components, devices, and users of CEN 17 Client Services.

Use of business email (or personal email if identified as business email by customer) is for routine contact in response to an IT service management issue/incident. For example, it will be used to communicate to a customer that an IT issue has been resolved.

The information found in the case management system is used to document, manage, and coordinate response to physical security, occupational safety, privacy, and data security incidents involving employees, contractors, visitors, members of the public and foreign nationals.

- 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.)

Security measures in place to ensure that information is handled properly include protections for data at rest and data in in transit. Data at rest is encrypted to ensure the confidentiality and integrity of the information. Data in transit is sent via encrypted tunnels using HTTPS . To ensure that users are handling the information properly, users are required to take Data Stewardship training annually and follow the Census Acceptable Use Policy.

**Section 6: Information Sharing and Access**

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies	X		
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	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:
	No, this IT system does not connect with or receive information from another IT system(s) authorized to

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

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

Class of Users			
General Public		Government Employees	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: <a href="https://www.census.gov/about/policies/privacy/privacy-policy.html">https://www.census.gov/about/policies/privacy/privacy-policy.html</a> . In addition, the following Notice and Consent Warning is display upon access to this IT system: <i>“You are accessing a United States Government computer network. Any information you enter into this system is confidential. It may be used by the Census Bureau for statistical purposes and to improve the website. If you want to know more about the use of this system, and how your privacy is protected, visit our online privacy webpage at http://www.census.gov/about/policies/privacy/privacy-policy.html.”</i> <i>“Use of this system indicates your consent to collection, monitoring, recording, and use of the information that you provide for any lawful government purpose. So that our website remains safe and available for its intended use, network traffic is monitored to identify unauthorized attempts to access, upload, change information, or otherwise cause damage to the web service. Use of the government computer network for unauthorized purposes is a violation of Federal law and can be punished with fines or imprisonment (PUBLIC LAW 99-474).”</i>	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the Case management application, individuals can determine how much PII to reveal.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Employee/contractor information in the database is automatically imported from CBS and cannot be declined at the CEN17 level.

- 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 the Case management application, individuals can determine how much PII to reveal.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Employee/contractor information in the database is automatically imported from CBS and cannot be declined at the CEN17 level.

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 are able to review/update information within the appropriate Census Bureau applications. In addition, by Privacy Act Request and FOIA Request.
	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:
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ____ July 9, 2019 ____ <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 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).

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
- 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 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.

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

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>  Commerce/Dept-25, Access Control and Identity Management System: <a href="http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html">http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html</a>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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:
---	---

	GRS 3.1, GRS 3.2, and 4.3
	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:
	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	X	Deleting	X
Other (specify):			

**Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level**

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. (*The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.*)

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: Combined data elements uniquely and directly identify individuals
X	Quantity of PII	Provide explanation: A serious or substantial number of individuals would be affected by loss, theft, or compromise of the PII collected, maintained, and/or disseminated.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, have little relevance outside the context.
X	Context of Use	Provide explanation:

		Disclosure of the act of collecting, and using the PII, or the PII itself is unlikely to result in harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.
X	Access to and Location of PII	Provide explanation: Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities.
	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.)

<p>PII/BII data at rest and in transit is vulnerable to potential attackers. To mitigate this risk 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:</p> <ul style="list-style-type: none"> <li>• Intrusion Detection   Prevention Systems (IDS   IPS)</li> <li>• Firewalls</li> <li>• Mandatory use of HTTP(S) for Census Bureau Public facing websites</li> <li>• Use of trusted internet connection (TIC)</li> <li>• Anti-Virus software to protect host/end user systems</li> <li>• HSPD-12 Compliant PIV cards</li> <li>• Access Controls</li> </ul>
--

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

<p>Yes, the conduct of this PIA results in required business process changes. Explanation:</p>
--

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.