

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



**Privacy Threshold Analysis
for the
CEN21 Human Resources Applications**

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau CEN21 Human Resource Applications

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

CEN21 applications are major application systems with several subsystem components. These IT systems provide support for internal and external customers in need of automated services for managing applicant/contractor suitability, personnel processing, time tracking, payroll processing, and other administrative activities. The systems are designed to meet the workforce needs of Census Bureau employees and contractors.

b) *System location*

The information collected and maintained by CEN21 IT computing systems is housed in the 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)*

CEN21 systems interconnect with other systems both internal and external such as:

- Department of Homeland Security (DHS) – personnel verification
- Department of the Treasury/HRConnect – HR data, payroll, bank routing data
- Federal Bureau of Investigation (FBI) – fingerprint, criminal records data
- Office of Personnel Management (OPM) – recruiting data, health benefits, flexible spending account data
- National Finance Center (NFC) – payroll, HR, awards and performance rating data
- Department of Commerce – webTA data

- Social Security Administration (SSA) – HR data
- Several external vendors (private sector)
 - Everbridge – employee/contractor emergency notification data
 - EQUIFAX – unemployment compensation data
 - LTC Partners – Federal Long Term Care Insurance data,
 - CornerStone Solutions – Recruitment/assessment data and
 - IndraSoft Inc (Fingerprint Vendor).

Tax data is also shared with the IRS, state and local municipalities, as required by law.

d) The purpose that the system is designed to serve

CEN21 is designed to serve the following purposes:

For administering Human Resources (HR) programs: The agency will use the information collected to administer Human Resources (HR) programs. For example, the system collects performance related information on employees, employees' supervisor, employee rating information, and comments related to performance. Once hired, the information is used to manage personnel and payroll records. The information in this system is vital in order to keep track of and disseminate Census Bureau employee's HR/payroll transactions.

The CEN21 IT system also collects/maintains data from USA Jobs job applicants, job offers, and collects employee-competency proficiency data (the knowledge, skills, and abilities) needed to perform.

For administrative matters: The information is used to run background investigations of applicants, which include members of the public, federal employees, contractors and foreign nationals, to provide staffing for the Census Bureau.

e) The way the system operates to achieve the purpose

CHEC: The Census Hiring and Employment Check (CHEC) system automates the electronic processing of personnel security data in support of background checks and employment suitability investigation for Census Bureau employees and contractors.

CHRIS: The Census Human Resources Information System (CHRIS) is a suite of workforce management applications. CHRIS is key in helping employees keep track of all human resources-related information such as emergency contact information, training history and personnel action history. Employees also use CHRIS to apply for telework and desk sharing.

CHRIS contains other components used by Human Resources Division and hiring managers such as Mixed Tour, the Electronic Hiring System (used to hire schedule A and veterans), the Census Awards Recognition System, and Performance Evaluation and Recognition System. HRD and Administrative Officers also use Entry on Duty and Accessions Forms Tracking for tracking the forms and onboarding status of employees. Personnel action requests are entered in the Personnel Action Request System and Employee Relations Cases

are managed and traced via the Employee Relations System. CHRIS also houses the time and expense system used to track the hours worked and expenses charged by Field Representatives working on current surveys. The Census Health System is also a component of the CHRIS system. Any services provided by the Census Health Unit to employees, contractors or other visitors in the building are charted and managed by Census Health Unit staff via CHS.

DAPPS: The Decennial Applicant Personnel and Payroll System (DAPPS) is a fully integrated human resources and payroll system that meets financial and regulatory reporting requirements for temporary decennial field staff. This web based enterprise-wide system supports the recruiting and applicant process, creating electronic certificates, hiring/rehiring staff, processing personnel actions, entering daily time & expense, running weekly payrolls, creating reports, and maintaining historical information.

Everbridge: A FEDRAMP authorized cloud service provider approved for use as the Census Bureau's official Emergency Notification System (ENS). Everbridge delivers a unified critical communication suite to the Census Bureau which allows the Census Bureau's Safety and Occupational Health office to communicate with employees quickly and effectively in the event of an emergency situation such as a weather related emergency, active shooter situation, etc. Everbridge is also used by the Lan Technology Support Office (LTSO) to send IT alerts and other important IT related information to Census Bureau employees who choose to opt in for the IT notifications through the CHRIS application.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

The different information types in the CEN21 information systems include:

- Employee and contractor workforce data including, but not limited to, first, middle, last name, home/work address, telephone numbers, email address, Social Security Number (SSN).
- Employee salary payments, tax and health benefits data
- Hours worked, expense reimbursements and payroll data
- Background investigation data including Fingerprints and criminal history
- Performance rating scores and dates and comments
- Award data (e.g., award type, award amount, award purpose and date)
- Employee language skills, education, ethnicity/race and disability status
- Employee personnel action history and training history
- Employee and contractor competency proficiency data
- Information about job applicants, hiring certificates, job offers (includes different categories of employees e.g., veterans, schedule A, interns)
- Applications for employees to apply for telework and desk sharing which include data such as name, grade, division, work phone number, supervisor.
- Employee relations case information related to grievances, EEO complaints and performance-related issues
- Patient health care records and other patient related information.

- Census bargaining unit status
- Retirement benefit data
- Employee/contractor emergency notification data

g) Identify individuals who have access to information on the system

Government employees and contractors

h) How information in the system is retrieved by the user

Information contained in the CEN21 information systems are available to authorized Census Bureau federal employees and contractors with need-to-know access to the applications. The information within the CEN21 systems is retrieved using authorized internal web applications, file servers and/or databases that are protected with a multi-layer security approach as identified in the selected security controls for the information systems within the CEN. Individual records are retrieved by name, employee number, or other personal identifier.

i) How information is transmitted to and from the system

Information is transmitted to and from CEN21 systems via web services, secure file transfer protocol (SFTP), Enterprise Service Bus (ESB) and Oracle JDBC Database links.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*
- 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). *Continue to answer questions and complete certification.*
- 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). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

- Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

- No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII.

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

DOC employees

National Institute of Standards and Technology Associates

Contractors working on behalf of DOC

Other Federal Government personnel

Members of the public

No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

SSN is required for tax reporting, enrollment for health/life insurance/long-term care/flexible spending benefits etc., background investigations, criminal background records, employee verifications through E-Verify, unemployment compensation and USA staffing through USAJobs.

Provide the legal authority which permits the collection of SSNs, including truncated form.

5 U.S.C. 301, 44 U.S.C. 3101, and 3309; 5 U.S.C. 7531-332
5 U.S.C., 5379, 5 CFR Part 537,
5 U.S.C. 1302, 2951, 3301, 3372, 4118, and 8347
5 U.S.C. 1104, 3321, 4305, and 5405
5 U.S.C. 3321, 4303, 7504, 7514, and 7543
5 U.S.C. 309, , 3109, 3302, 3304, 3305, 3306, 3307, 3313, 3317, 3318, 3319, 3326,
4103, 4723, 5532, and 5533
5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11)
5 U.S.C. Chapters 11, 33, and 63

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.