Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
ADEP Economic Applications Division
Windows Applications System

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/EAD Windows Applications System

Unique Project Identifier: 00600040070

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).

Introduction: System Description

The ADEP Economic Applications Division (EAD) Windows Applications IT system is hosted at Census Bureau facilities and comprised of four main types of applications:

1. Data collection through Census Bureau funded censuses and surveys is done for state and local governments, libraries, prisons and other institutions considered public entities[1]. In addition to Census Bureau funded surveys, data collection is done on a reimbursable basis for other sponsors such as the Department of Justice, the National Center for Education Statistics, The Institute of Museums of Museums and Library Services, the Office of Management and Budget, the Department of Education, and the National Science Foundation. (Note: Some data collection is provided by OCIO Centurion. Centurion is the Census Bureau enterprise solution for the on-line collection of survey or census responses.)
2. Data processing is done on information collected by ADEP Economic Applications Division (EAD) Windows Applications System applications, data collected by OCIO Centurion, as well as data obtained from other internal Census Bureau sources. The extent of data processing is dependent on the requirements of the individual project.
3. Data dissemination is done in a variety of ways depending upon the owner of the data and the confidentiality of the data. All data owned by entities external to the Census Bureau is disseminated consistent with the directives of the data owner. Information that is

[1] Public entities for this document are federal, state, and local governments; government funded entities; and not-for-profits. Some entities included in this PIA, such as prisons and correctional facilities, may be privately owned. For the sake of simplicity, all of these entities will be referred to as "public entities".

classified as publicly accessible can be posted to public facing internet sites. Information that requires some level of confidentiality has access restricted through identification and authentication functionality.

4. Analysis/Research - Data Analysis is performed, for approved projects only, to create the results of data analysis which includes, but is not limited to, data products.

(a) Whether it is a general support system, major application, or other type of system
ADEP Economic Applications Division (EAD) Windows Applications System is a general support system.

(b) System location
ADEP Economic Applications Division (EAD) Windows Applications System servers are physically located in 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)
ADEP Economic Applications Division (EAD) Windows Applications System Windows Applications System interconnects with the following systems:

- OCIO Data Communications – provides telecommunications, network infrastructure, and support
- ADEP Economic Census and Surveys and Special Processing – provides Oracle databases and support
- OCIO Network Services – provides server and operating systems and support
- OCIO Client Services – provides desktop and laptop support
- OCIO Enterprise Applications – provides enterprise level applications/support (ex. SAS) and MS SQL Server databases and support

(d) The purpose that the system is designed to serve
ADEP Economic Applications Division (EAD) Windows Applications System has five primary purposes: administrative matters, the administration of human resource programs, the promotion of information sharing initiatives, employee and/or customer satisfaction, and statistical purposes.

(e) The way the system operates to achieve the purpose(s)
Based on the information in Section 4: Purpose of the System

- *For administrative matters* and *for administering human resources programs* – one application subcomponent is used to track prospective Census Bureau employees through the interview process. All information specific to the individual is the content of the resume which the individual provided as a part application process.
- *To promote information sharing initiatives* – there are three types of PII/BII that are disseminated (i.e., shared) by ADEP Economic Applications Division (EAD) Windows Applications System.
    i. Information that falls under Title 13 section 9b which does not require the confidentiality of most Title 13 data. This data is made available through

public facing websites and/or file transfers. This data is not considered confidential although it falls under the classification of PII/BII.

ii. Information that is required to be collected and disseminated by federal law or policy. For example, recipients of $750,000 or more in federal grants or required to report how the funds were spent and that information must be disseminated to the public. This data is made available through public websites and/or file transfers. This data is not considered confidential although it falls under the classification of PII/BII.

iii. Information that is collected on behalf of a sponsor from a federal agency, internal or external to the Census Bureau. This data is considered Title 13 and/or confidential and is shared only through secure file transfers. It is not disseminated to the public.

- *For employee or customer satisfaction* – this information is collected as a part of feedback from application and/or data users. This information is not disseminated to the public and is used only to improve applications and/or data products.
- *Statistical purposes* – one of the primary purposes for collecting and maintaining PII/BII is for statistical (i.e., analysis and research) purposes.

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

- Census and Survey data,
  - Identifying Numbers (IN): Employer ID
  - General Personal Data (GPD): Name
  - Work-Related Data (WRD): Address, Telephone Number, and Email Address.

  This information is collected as a part of identifying the respondent to a census or survey interview. Usage: This information is occasionally used to contact the respondent for additional information or clarification. This information is not disseminated unless the entire response is considered 'public content'. The respondent/person that the PII/BII is about is an employee or representative of a public entity.
- The following information is collected as a part of a prison survey:
  - General Personal Data (GPD): Gender
  - General Personal Data (GPD): Race/Ethnicity
  - General Personal Data (GPD): Date of Birth

  This information is collected about prison employees and/or inmates for statistical purposes and is never disseminated at an individual level. Name is not collected, and the Census Bureau lacks the information to tie the collected information to an individual. In addition, the Census Bureau only uses this information to generate statistical analyses and does not release the original information.
- Statistical research and analysis includes all data types in Identifying Numbers (IN), General Personal Data (GPD) and Work-Related Data (WRD) from Title 13, Title 13 section 9b, and Title 26 data. This information is analyzed for research purposes which may result in the creation of data/information productions. The Census Bureau never releases the original PII/BII information.
- Interview Tracking data,
  - General Personal Data (GPD): Name, Home Address, Telephone Number, Email Address, Education, and Military Service

  - Work-Related Data (WRD): Occupation, Job Title, Business Address, Salary, and Work History

  This information is collected/maintained when a person submits a resume and/or job application for a job opportunity. Usage: This information is used as a part of the interview process and is never disseminated to the public. The PII is for a job applicant who may be a federal employee, a federal contractor, or member of the public.
- System Administration/Audit Data (SAAD): User ID, IP Address, and Date/Time of Access. This information is required as a part of the Census Bureau IT Security Program Policy that is based on NIST SP 800-53. Usage: This information is used as a part of the application monitoring (see NIST SP 800-53 for more information on the use of audit logs). Audit logs are generated for the user of the application who can be a federal employee, a federal contractor, or a member of the public.

(g) Identify individuals that have access to the system

- U.S. Census Bureau employees and contractors – many Census Bureau approved projects require that Census Bureau employees have direct access to information in order to analyze and/or process the information. All employees with this type of access have a work related need to have access to the information and have met all training and requirements.
- Government employees from other federal agencies and state, local, and/or tribal agencies – some employees/users from other federal agencies or state, local, and/or tribal agencies require direct access to information. These employees/users must be participants in a project approved by both agencies and then access the information by use of valid identification and authentication credentials.
- Public and private sector - through search functionality, users can directly access individual responses to specific surveys. These responses contain only public content as described. Information sharing with the private sector and public is done only with a specific type of PII/BII. The PII/BII that is shared is either classified under Title 13 section 9b and/or is specific to an individual in their role as government employee rather than in their role as private citizen. For example, the person's name, government phone number, and government address can be a part of information sharing. A county government name, phone numbers, and address uniquely identify that government making it Business Identifiable Information, however, this information is available to the public and can be shared. The type of information described here is often referred to as public content.

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

Information retrieval by the user is dependent on the type of application:

- For data collection applications, respondents access their data through a response identifier which identifies the entity or the person reporting. Application administrators retrieve response data based on the response identifier and retrieve user related information based on the user ID.
- For data processing applications, users/analysts retrieve the data based on identifiers that uniquely identify an entity[2].

[2] A record may be associated with an individual, business, or government.

- For data dissemination applications that require user log on, users retrieve the data based on identifiers that uniquely identify the entity.
- For research/analysis projects, users do not retrieve data based on identifiers that uniquely identify an entity.

(i) How information in the system is transmitted to and from the system

The exact type of information transmission to and from an application is dependent on the type of application:

- For data collection applications, data transmission leverages TLS 1.2 on the public facing websites. Databases are initialized internally before making the data collection application available to respondents. Encryption is required on all transmissions.
- For data processing applications, the databases are initialized by automated processes. All applications are available only inside the firewall and encryption is required on all transmissions.
- For data dissemination applications, data transmission leverages TLS 1.2 on the public facing websites. Encryption is required on all transmissions.
- For research/analysis projects, all data are available only inside the firewall and encryption is required on all transmissions.

Questionnaire:

1. Status of the Information System

1a. 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 or 01-2017). *Continue to answer questions and complete certification.*

__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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X_ No. This is not a new information system.

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):			

__X_ 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.)."

__X_ 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."

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

__X_ DOC employees
__X_ Contractors working on behalf of DOC
__X_ Other Federal Government personnel
__X_ 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. Not Applicable
Provide the legal authority which permits the collection of SSNs, including truncated form. Not Applicable

__X_ 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?

__X_ 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.

__X_ 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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

___X___ I certify the criteria implied by one or more of the questions above **apply** to the ADEP Economic Applications Division (EAD) Windows Applications System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner (SO) Name: Sumit Khaneja Office: Chief, Economic Applications Division Phone: 301-763-7623 Email: Sumit.Khaneja@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: SUMIT KHANEJA Digitally signed by SUMIT KHANEJA Date: 2021.11.29 13:26:32 -05'00' Date signed: _____	**Business Authorizing Official (BAO)** Name: Nick Orsini Office: Associate Director for Economic Programs Phone: 301-763-6959 Email: Nick.Orsini@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: NICK ORSINI Digitally signed by NICK ORSINI Date: 2021.12.07 14:26:43 -05'00' Date signed: _____
Chief Information Security Officer (CISO) Name: Beau Houser Office: Chief, Office of Information Security Phone: 301-763-1235 Email: Beau.Houser@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2021.12.02 09:37:42 -05'00' Date signed: _____	**Agency Authorizing Official (AAO)** Name: Luis Cano Office: Chief Information Officer Phone: 301-763-3968 Email: : Luis.Cano@census.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2021.12.02 11:09:33 -05'00' Date signed: _____
Bureau Chief Privacy Officer (BCPO) Name: Byron Crenshaw Office: Chief, Privacy Compliance Branch Phone: 301-763-7997 Email: Byron.Crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.01.06 16:12:58 -05'00' Date signed: _____	**Privacy Act Officer (PAO)** Name: Byron Crenshaw Office: Chief, Privacy Compliance Branch Phone: 301-763-7997 Email: Byron.Crenshaw@census.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.01.06 16:13:30 -05'00' Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.