Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
OCIO ADSD CIB Administrative Systems Vol. II

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/OCIO/ADSD/CIB Administrative Systems Vol. II

Unique Project Identifier: 006-000403600

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: *Provide a brief description of the information system.*

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).

Office of the Chief Information Officer / Applications Development & Services Division / Commercial Off the Shelf (COTS) Integration Branch (OCIO/ADSD/CIB) Administrative Systems Vol. II, encompasses a wide variety of Administrative Business Solutions. These applications are used throughout the U.S. Census Bureau provide products and services that ensure a productive and safe work environment. Examples of these systems can be found in section a. The tools included are:

- Electronic records management system used to track the location and retention periods of legacy and CRI Paper to digital records
- Enterprise reservation system for federal employees and contractors to reserve conference, training, meeting, and desk workspaces.
- Conference reservation system used to manage reservations for conference rooms, training rooms, and the auditorium.
- Library management system gives people the ability to view library collections from anywhere in the world
- Environmental monitoring system is a software/hardware solution to monitor the temperature / humidity & flooding
- Mail metering system is a collection of mail metering stations located at Census headquarters, regional offices, and the National Processing Center that are used to place postage on outgoing United States Postal Service (USPS) mail pieces or parcels.
- Correspondence oversight & tracking tool is used to route and manage permanent record correspondence between Congress, the director's office, and program areas within the Census Bureau.

Address the following elements:

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

Administrative Systems Vol. II is a collection of major applications.

b) System location

Most of the Administrative Systems Vol. II applications are hosted at Census Bureau Headquarters at the Bowie Computer Center. The ones that are not hosted at Census Bureau locations are cloud services and the cloud vendor headquarter locations are listed below.

- Dublin, Ohio
- Seattle, Washington
- Stamford, Connecticut

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

Administrative Systems Vol. II interconnects with OCIO Data Communications, OCIO Network Services, and OCIO Enterprise Applications for authentication/infrastructure purposes.

d) The purpose that the system is designed to serve

Administrative Systems Vol. II is used to identify users, authorize users, and control to applications.

e) The way the system operates to achieve the purpose

Administrative Systems Vol. II applications are used throughout the U.S. Census Bureau in accomplishing its mission in an efficient manner. The program areas' business solutions provide timely, relevant, high-quality products and services, and ensure a productive and safe work environment to support the U.S. Census Bureau and its employees in meeting and exceeding the Agency's mission, strategic goals and objectives.

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

Administrative Systems Vol. II maintains very little PII. The PII maintained within are name, employee id, work email address, key card number, work address, and work phone number.

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

U.S. Census Bureau government employees and contractors have access to Administrative Systems Vol. II.

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

Administrative Systems Vol. II. information can be retrieved by an identifier such as name or employee id. Information contained in the information systems are available to authorized U.S. Census Bureau federal employees and contractors.

i) How information is transmitted to and from the system

Information is transmitted between Administrative Systems Vol II. and Census Bureau enterprise systems. Components use enterprise supported databases. Administrative Systems Vol. II also uses enterprise support Lightweight Directory Access Protocol (LDAP) services for user authentication, including Single Sign On. These connections are all encrypted. Administrative Systems Vol. II also receives software updates from external vendors using the HTTPS encrypted protocol. Content data will be preloaded and updated in the reservation system with Low rated HR Data Feed from the Census Identity Management Systems (IDMS); the Low rated HR Data Feed is sent encrypted via a SFTP process. There's an additional connection with a vendor where electronic funds are downloaded to our postal meters. This connection is also encrypted as required by the United States Postal Service.

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.*

_X_ 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): Inline desktop signage device (badge reader) for confirmation a location is free, reserved, being used.					

____ 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. *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.)."

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

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

_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?

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

__ X__No, the user ID is the only PII collected, maintained, or disseminated by the IT system(s).

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___ The criteria implied by one or more of the questions above **apply** to the OCIO/ADSD/CIB Administrative Systems Vol. II and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ 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.

Information System Security Officer Name: Deanna Fleetwood Office: Office of Information Security Phone: 202-603-8275 Email: Deanna.christine.fleetwood@census.gov Signature: DEANNA FLEETWOOD Digitally signed by DEANNA FLEETWOOD Date: 2023.03.07 09:49:10 -05'00' Date signed:	**Chief Information Security Officer** Name: Beau Houser Office: Office of Information Security Phone: 301-763-1235 Email: Beau.Houser@census.gov Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2023.03.07 11:14:17 -05'00' Date signed:
Privacy Act Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301.763.7997 Email: Byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.03.13 16:42:52 -04'00' Date signed:	**Agency Authorizing Official** Name: Luis J. Cano Office: Office of the Chief Information Officer Phone: 301.763.3968 Email: luis.j.cano@census.gov Signature: Gregg Bailey Digitally signed by Gregg Bailey Date: 2023.03.10 15:06:28 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Byron Crenshaw Office: Policy Coordination Office Phone: 301.763.7997 Email: Byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2023.03.13 16:44:54 -04'00' Date signed:	