Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
OCIO Office of Information Security (OIS) Systems

U.S. Department of Commerce Privacy Threshold Analysis

U.S. Census Bureau/OCIO Office of Information Security (OIS) Systems

Unique Project Identifier:

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 (OCIO) Office of Information Security (OIS) Systems employ several security technologies used to manage and protect the security posture of the Census Bureau. The security technologies provide the agency with capabilities including: the enterprise Governance, Risk & Compliance (GRC) system for the documenting and storing of System Security Plans (SSPs) for Census Bureau-wide information systems; system vulnerability and compliance scanning systems which enables the organization to monitor the network, systems, and applications for security vulnerabilities; and a database security system which helps the organization secure enterprise databases, big data stores and the processing of forensic data to help with security investigations.

Information is only collected from within the Census internal network. Census Bureau end points, servers, network and storage devices have to be configured to send security data to data aggregation points.

The personally identifiable information (PII) maintained in OIS Systems is limited to account information such as User ID, names, JBID's and work email addresses of federal employees and contractors that access Census Bureau resources.

Address the following elements:

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

OIS Systems consists of major applications.

b) System location

The Census Bureau's Bowie Computer Center (BCC) in Bowie, Maryland.

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

Interconnections for OIS Systems are restricted to the collection of security data from all Census systems including network traffic monitoring and analysis, and security scan data from Census Bureau servers, network devices, and storage solutions.

d) The purpose that the system is designed to serve

OIS Systems employs a number of security tools used to manage and protect the security posture of the agency. Security tools provide alerts on malicious traffic or actions, document system security plans for Bureau-wide information systems, conduct vulnerability and compliance scans, enforce database security, and process forensic data to help with security investigations.

e) The way the system operates to achieve the purpose

OIS Systems has a number of IT systems that help alert Census Bureau staff on malicious traffic or actions, document system security plans for Census Bureau-wide information systems, conduct vulnerability and compliance scans, enforce database security, and process forensic data to help with security investigations.

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

The personally identifiable information (PII) collected is in reference to federal employees and contractors that use Census Bureau IT systems. User ID's, JBID's, IP addresses, and date and time of access are collected for cyber security purposes including network monitoring and analysis, and vulnerability scanning data.

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

U.S. Census Bureau government employees and contractors.

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

The PII maintained in OIS Systems is limited to account information such as User ID, names, JBID's and work email addresses of federal employees and contractors that access Census Bureau resources. These are the PII that is used to retrieve information in the system.

Access to OIS Systems must be approved and PII is restricted via access control mechanisms and limited to user job responsibilities.

i) How information is transmitted to and from the system

Information is only collected from within the Census internal network. Census Bureau end points, servers, network and storage devices have to be configured to send security data to data aggregation points. Data is encrypted via Federal Information Processing Standards (FIPS) 140-2 cryptographic mechanisms.

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.*

__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. *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
__X__ 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?

__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__ The criteria implied by one or more of the questions above **apply** to the OCIO OIS Systems 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 OCIO OIS Systems and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: Christopher Wright Office: Office of Information Security Phone: 202-893-5012 Email: Christopher.d.wright@census.gov Signature: CHRISTOPHER WRIGHT Digitally signed by CHRISTOPHER WRIGHT Date: 2022.02.03 09:25:45 -05'00' Date signed: _____	**Chief Information Security Officer** Name: Beau Houser Office: 3K106 Phone: 301-763-1235 Email: beau.houser@census.gov Signature: BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2022.03.08 10:03:36 -05'00' Date signed: _____
Privacy Act Officer Name: Byron Crenshaw Office: 8H021 Phone: 301-763-7997 Email: Byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.03.10 11:31:26 -05'00' Date signed: _____	**Authorizing Official** Name: Luis J. Cano Office: Chief Information Office Phone: (301) 763-3968 Email: luis.j.cano@census.gov Signature: LUIS CANO Digitally signed by LUIS CANO Date: 2022.03.01 13:14:44 -05'00' Date signed: _____
Bureau Privacy Officer Name: Byron Crenshaw Office: 8H021 Phone: 301-763-7997 Email: Byron.crenshaw@census.gov Signature: BYRON CRENSHAW Digitally signed by BYRON CRENSHAW Date: 2022.03.10 11:31:59 -05'00' Date signed: _____	