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

Privacy Impact Assessment
for the
OCIO Office of Information Security (OIS) Systems

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.03.29 11:10:58 -04'00'   3/29/24

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/OCIO Office of Information Security (OIS) Systems

Unique Project Identifier:

<u>Introduction</u>: System Description

Provide a brief description of the information system.

Office of the Chief Information Officer (OCIO) Office of Information Security (OIS) Systems employ multiple security technologies used to manage and protect the security posture of the Census Bureau. The security technologies provide the agency with a variety of security capabilities including:
1) Vulnerability scanning systems.
2) Compliance scanning systems.
3) Web-application scanning systems.
4) Intrusion Detection Systems (IDS).
5) Intrusion Prevention Systems (IPS).
6) Packet capture systems.
7) Endpoint detection and response (EDR).
8) Security Information and event management system (SIEM).

Information is collected from within the Census Bureau internal network. Census Bureau end points, servers, network, and storage devices must 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 names, JBID's (user ids) 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 are general support systems.

(b) System location

The systems reside at the Census Bureau's various Computer Centers and in the cloud.

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

OIS Systems has a number of IT systems that help alert Census Bureau staff on malicious traffic or actions, conduct vulnerability and compliance scans, and process forensic data to help with security investigations. Descriptions of each tool are as follows:

1. Vulnerability scanning systems provide the Census Bureau with the ability to perform asset discovery, continuous monitoring, provide vulnerability remediation recommendations and vulnerability identification.
2. Compliance scanning systems provide the Census Bureau with the ability to ensure that our Enterprise Secure Configurations Benchmark controls are compliant, according to industry best practices.
3. Web-application scanning systems provide the Census Bureau with the ability identify security weaknesses and drive proactive mitigation of publicly accessible and internal web applications by checking for known vulnerabilities and weak configurations.
4. Intrusion Detection Systems (IDS) provide the Census Bureau with the ability to detect vulnerability exploits and attacks against and within the census networks, and to provide validation that security rules are working as designed.
5. Intrusion Prevention Systems (IPS) provide the Census Bureau with the ability to prevent active attacks, exploits and malware attempting to access systems.
6. Packet capture systems provide the Census Bureau with the ability to retain network traffic to assist in the investigation and response to network security events and incidents.
7. Endpoint detection and response (EDR) provide the Census Bureau with the ability to monitor workstations, laptops and servers and respond to cyber threats and gather forensic information to support investigations of security events and incidents.
8. Security Information and event management system (SIEM) provide the Census Bureau with the ability to capture system logs and events in a central location and provide capabilities to detect, analyze and respond to events on the networks.

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

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

(f) 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.

(g) Any information sharing

The information in OIS Systems is shared with the Bureau of the Census Cybersecurity Center (CCC) and with the Department of Commerce Enterprise Security Operations Network (DOC ESOC). After information is shared with the DOC ESOC, it may also be shared with the Cybersecurity & Infrastructure Security Agency (CISA).

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

5 U.S.C. 301 (Departmental Regulations); and 44 U.S.C 3101 (Records Management).

(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.

__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.

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.)*

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

General Personal Data (GPD)					
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		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	

c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2   Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
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.

The accuracy of the information is ensured through continuously maintaining and verifying compliance with agency privacy and security requirements through ongoing information system monitoring and analysis that includes automated scripts, testing and data integrity rules that trigger notifications and system email notifications.

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.)*

Purpose			
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).

> OIS Systems data will be used in the following ways:
>
> For administrative matters:
> The PII collected is in reference to federal employees and contractors that use Census Bureau IT Systems. 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.

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.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization, accidental leaks, and misuse of information. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Census Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

OIS Systems security tools are Census Bureau internal use applications. There is no dialup connectivity or public internet access to the applications. All users connect to the tools via the Census Bureau's internal high-speed network using FIPS 140-2 validated encrypted communication. End-user and administrator external access to these systems is allowed through SecurID and VDI per Census Bureau policy.

In addition, 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 hypertext transfer protocol secure (HTTPS) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- 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 and a security operations center to monitor all Census IT system on a 24/7/365 basis.

The information in OIS Systems is handled, retained, and disposed of in accordance with appropriate federal record schedules.

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 CCC		X
DOC bureaus	X DOC ESOC		
Federal agencies	X CISA		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2   Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3   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: OIS Systems interconnects with all Census systems. OIS Systems employs a number of enterprise security tools used to manage and protect the security posture of Census systems. Security tools provide alerts on malicious traffic or actions, conduct vulnerability and compliance scans, enforce database security, and process forensic data to help with security investigations of Census IT assets. OIS Systems uses a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. There is also mandatory security training for system users regarding appropriate handling of information, automatic purging of information in

	accordance with the retention schedule and other agency security requirements. The census Bureau also deploys a Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4   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: https://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: Notice that PII is collected, maintained, or disseminated in the system is provided by the login banner to the network.
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Federal Requirements subject users to provide PII/BII. Users are required to agree to in order to be employed at the Census Bureau.

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: Users must consent to all uses of their PII to be employed with the Census Bureau.

	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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 may review/update PII via the applicable human resources applications.
	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: Only authorized government/contractor personnel are allowed to access PH/BII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
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): _____7/26/2023_____ ☐ 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).*

Census Bureau Information technology systems employ a multitude of layered security controls to protect PII 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 I IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

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 that contains, transmits, or processes 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. Census also deploys a DLP 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)?

    __X__   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. *(list all that apply)*:
	COMMERCE/DEPT-27, Investigation and Threat Management Records: https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-27.html
	COMMERCE/DEPT-25, Access Control and Identity Management System: https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	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: General Record Schedule 3.1 - General Technology Management Records General Record Schedule 3.2 - Information Systems Security Records
	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:
X	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.)*

Disposal			
Shredding		Overwriting	
Degaussing		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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Data elements are not directly identifiable alone but may indirectly identify individuals.
X	Quantity of PII	Provide explanation: A limited number of individuals would be affected by loss, theft, or compromise.
X	Data Field Sensitivity	Provide explanation: PII collected and maintained is non-sensitive which is unlikely to result in harm to individuals.
X	Context of Use	Provide explanation: Disclosure of PII itself is unlikely to result in harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: PII collected is required to be protected in accordance with 13 U.S.C. section 9.
X	Access to and Location of PII	Provide explanation: PII is located on computers and other devices on a network controlled by the Census Bureau. Access is limited to certain populations of the Census Bureau's workforce with a work related need to know.
	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.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible. In addition to the security protocols already described in this assessment, the Census Bureau limits access to sensitive information to sworn employees who have an authorized business need to know.

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
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.