Template Version Number: 01-2021

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

Privacy Impact Assessment
for the

OCIO Application Development and Services Division (ADSD) Enterprise Development Tools Support Branch (EDTSB)

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

TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2024.10.11 13:22:53 -04'00' for Charles Cutshall 8/28/2024

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 Application Development and Services Division (ADSD) Enterprise Development Tools Support Branch (EDTSB)

Unique Project Identifier: [Number]

Introduction: System Description

Provide a brief description of the information system.

The Office of the Chief Information Officer (OCIO) Application Development and Services Division (ADSD) Enterprise Development Tools Support Branch (EDTSB) PIA includes primary tools managed by the Enterprise Development Tools Support Branch. EDTSB provides tools for use by the Census Bureau enterprise customers (the customers utilizing these tools are all Census Bureau employees, which includes federal employees and special sworn contractors). While the tools are authorized to handle Title 13 and Title 5 data, they will not be storing survey response/raw data. The primary tools managed by EDTSB are:

1. Project management and ticketing software
2. Source code repository
3. Document management system

The **project management and ticketing software** is a robust system that provides essential enterprise services and leverages the OCIO Data Communications enterprise authentication tool for secure access. The system is designed to help teams of all sizes plan, track, manage, and report on projects and work efficiently across the entire software development lifecycle.

The system streamlines project management, issue tracking, and collaboration through its versatile features:

1. Project Planning: Teams can create and organize tasks, set priorities, and establish deadlines using customizable workflows and boards.
2. Issue Tracking: The system allows for detailed issue creation, assignment, and tracking, enabling teams to manage bugs, feature requests, and support tickets effectively.
3. Agile Methodologies: The software supports both Scrum and Kanban methodologies, offering sprint planning, backlog management, and burndown charts.
4. Reporting and Analytics: The system provides real-time reporting and analytics systems to help teams monitor progress, identify bottlenecks, and make data-driven decisions.
5. Customization: Teams can tailor system to fit their specific needs through custom fields, workflows, and project templates.

The EDTSB system administration team manages and administers the project management and ticketing software, making it available across the enterprise. EDTSB handles user provisioning, permissions, and overall system maintenance to ensure optimal performance and security.

While the system does not explicitly request Personally Identifiable Information (PII) or Titled data, such information may be entered into the system by Census Bureau employees (customers) in tickets for purposes such as resolving software issues or describing specific user scenarios. To maintain data privacy and security, only specific teams with proper authorization and a business need-to-know have access to the data within the system.

Tickets are submitted through an intuitive, user-friendly Graphical User Interface (GUI). This interface allows users to easily create, view, and update tickets without requiring technical expertise. Importantly, all ticket-related work, including submission, updates, and resolution, occur entirely within the system. This containment ensures that sensitive information and project data remain within the system's secure environment, reducing risk of data

leaks or unauthorized access. The self-containment nature of the software also streamlines the workflow, as team members can access necessary information and perform required actions without leaving the system.

The ticketing process in the system typically follows these steps:

1. Ticket Creation: Users create tickets describing tasks, bugs, or feature requests.
2. Triage: Tickets are reviewed, categorized, and prioritized by project managers or team leads.
3. Assignment: Tickets are assigned to appropriate team members.
4. Work in Progress: Assignees update the ticket status as they work on the ticket.
5. Review: Completed work is reviewed by peers or stakeholders.
6. Resolution: Once approved, the ticket is marked as resolved.
7. Closure: After final verification, the ticket is closed.

Throughout this process, the system facilitates communication between team members, stakeholders, and customers, ensuring transparency and efficient project management.

The **source code repository system** is a modern source code version control and configuration management system. It is a web-based platform that facilitates version control and collaborative software development. It allows developers to manage and track changes in their code, coordinate work with others, and host repositories for projects. Titled data will not be stored in the code repository.

The **document management system** is a team collaboration and team product documentation system. It is primarily used for creating, sharing, and collaborating on content. It is often employed for documentation, project planning, and team collaboration, providing centralized spaces for teams to work together on documents, wikis, and other content.

Address the following elements:

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

General Support System

(b) System location

The three systems are located at the Census Bureau Computer Center located 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)

OCIO ADSD EDTSB systems interconnects with infrastructure services at the U.S. Census Bureau. This includes OCIO Data Communications for authentication/ telecommunication purposes, OCIO Network Services for server/storage, OCIO Client Support Division (CSD) for laptops and workstations, and OCIO Enterprise applications for database support.

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

The EDTSB PIA consists of three primary systems:

1. **Project Management and ticketing software**: The project management and ticketing software is used for administrative matters, administering human resources programs, and for statistical/research purposes. The software operates by allowing teams across the Census Bureau to plan, track, and manage their work using an agile framework. Users can create and prioritize tasks, track the progress of work through customizable workflows, and collaborate with team members. While this system does not explicitly ask for PII, PII may reside in the tickets. E.g. UserID, name, and email.

   Tickets are submitted through an intuitive**,** user-friendly Graphical User Interface (GUI). This interface allows users to easily create, view, and update tickets without requiring technical expertise. Importantly, all ticket-related work, included submission, updates, and resolution, occurs entirely within the system. This containment ensures that sensitive information and project data remain within the system's secure environment, reducing risk of data leaks or unauthorized access. The self-containment nature of the software also streamlines the workflow, as team members can access necessary information and perform required actions without leaving the system.

   The ticketing process in the system typically follows these steps:

   1. Ticket Creation: Users create tickets describing tasks, bugs, or feature requests.
   2. Triage: Tickets are reviewed, categorized, and prioritized by project managers or team leads.
   3. Assignment: Tickets are assigned to appropriate team members.
   4. Work in Progress: Assignees update the ticket status as they work on the ticket.
   5. Review: Completed work is reviewed by peers or stakeholders.
   6. Resolution: Once approved, the ticket is marked as resolved.
   7. Closure: After final verification, the ticket is closed.

   The data maintained for *administrative purposes/administering human resources programs* relates to the Census Bureau's Human Resources Division's use of the ticketing system for issue tracking purposes; this pertains to federal employees/ contractors. An HR-related example use case of this system includes a customer submitting a ticket that they are separating from the government; the ticket may include their resignation letter as an attachment. The resignation letter could include PII such as name, address, etc. Another HR-related use case is that an individual is not seeing their performance plan in the authorized system. Their ticket could include a copy of the performance plan as an attachment. The authorized program area handling the matter can respond/comment within the ticket.

   The data maintained for *statistical and research purposes* relates to the use of the ticketing system for software defect resolution. A survey program area related example includes an

employee manually entering respondent information into a ticket for defect resolution purposes. When a problem or discrepancy is encountered within an application or database, a tester will create a defect/issue with a full description of what happened during testing along with steps on how to reproduce the reported defect. The testers will communicate by using comment threads until a resolution is reached and the defect is verified/closed.

The description and comment section of a defect should include information regarding the application being executed, and any applicable environment/database/tables being used. In addition, all relevant documentation such as release notes and software specifications, and data input and/or output. If the data input or output, includes any PII or Title 13 data, that information is communicated in a separate email via Kiteworks (email encryption service) or an encrypted message via regular email.

Examples of data may include data entered via the Internet Self Response instrument or data collected using software systems for field data collection operations. Other data inputs may include data that is manually extracted from the OCIO Enterprise Data Lake (EDL).

For 2030 Census, there are plans to use the project management and ticketing software in a similar manner. The software will be used to house the 2030 Census stakeholder level requirements, business threads, and test cases. In like manner, the software will be used to house, track, and process all program level defects identified during program level testing. The same types of data as described above are expected to be used for 2030 Census.

2. **Source code repository system**: The source code repository system is used for *administrative matters*. Internal Census Bureau teams use the underlying version control system to help track changes in the source code. Developers can create branches to work on specific features or fixes independently. The system provides project boards to visualize and manage work. They can be customized to fit various project management methodologies. The source code repository system contains very minimal PII such as UserID, name, and email.

3. **Document management system**: The document management system is used *to promote information sharing initiatives*. Internal Census Bureau teams use this system to create, organize, collaborate, and share documentation. This includes projects, plans, meeting notes, and other relevant information. It allows dedicated spaces and pages for projects. Teams can structure information hierarchically, making it easy to navigate. This system will also be used to provide dashboard metrics and reporting for management. The document management system will be approved for Titled data and PII. Any upload/download of documents is done manually and the capability to block downloads also exists. An example use case for this system would include the use of test and live address data files in support of

the 2030 Census; this could also include relevant information about specific addresses. The types of PII collected and maintained by this system include, UserID, name, and email.

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

In all three EDTSB systems, information can be retrieved by JBID.

(f) How information is transmitted to and from the system

Data in transit is encrypted with Transport Layer Security and storage is in an encrypted Storage Area Network (SAN) managed by OCIO Computer Services Division Operating System (OS) Services.

(g) Any information sharing.

The EDTSB project management and ticketing software will share internally with the EDTSB document management system and EDTSB source code repository system. These EDTSB systems do not share information with other IT systems external to EDTSB.

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

For survey-related data within EDTSB systems:

13 U.S.C. Sections 8(b), 131, 161, 141, 182, and 193.

For HR-related data within the EDTSB systems:

Title 44 U.S.C. 3101

5 U.S.C. 3321 and Executive Order 9397, as amended by 13478, 9830, and 12107

(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. 9/30/2024

_X_ 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.

____ 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*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: SSN is not specifically requested by the EDTSB project management/ticketing system however, the HR system administrators may have access to the social security number because it was submitted by a customer within a ticket.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify): The only GPD requested by the ticketing system is UserID, name and					

email; however, the HR system administrators may have access to the other PII items checked above because it was submitted by a customer within a ticket.

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

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): Respondent information may be manually entered into a ticket for defect resolution purposes.					

2.3 Describe how the accuracy of the information in the system is ensured.

For the project management and ticketing system, information is input by customers (Census Bureau employees); the customers would be responsible for the accuracy of their data.

For the document management repository, information is input by customers (Census Bureau employees); the customers would be responsible for the accuracy of their data. The system ensures accuracy by limiting the collaboration to only authorized individuals with a need to know. Security measures can also be put in place to make documents read only and block downloads as needed.

While the systems are in use, the data is accessible only to users that are authorized to use the data. The initial Authorization to Operate (ATO) and the Information Systems Continuous Monitoring program provides an ongoing monitoring of data accuracy as maintained by security controls derived from NIST 800-53 Rev 5. System and Communications (SC) provides Protection of Policy and Procedures, Application Partitioning, Information in Shared Resources, Denial of Service, Information System Boundary, Transmission Confidentiality & Integrity, and Cryptographic Protection. In addition, System and Information Integrity (SI) provides Flaw Remediation Protection, Malicious Code Protection, Inbound and Outbound Communications Traffic monitoring protection, System-Generated Alerts, etc.

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	X
For administrative matters	X	To promote information sharing initiatives	X
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): For statistical purposes (i.e., Censuses/Surveys).			

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).

EDTSB systems are enterprise systems, available to program areas within the Census Bureau for program management purposes.

Project Management and ticketing software

The PII maintained for administrative purposes and for administering human resources programs: The data maintained for administrative purposes/administering human resources programs relates to Human Resources' use of the ticketing system for issue tracking purposes; this pertains to Census Bureau employees, which includes federal employees and contractors. An HR-related example use case of this system includes a customer submitting a ticket that they are separating from the government; the ticket may include their resignation letter as an attachment. The resignation letter could include PII such as name, address, etc. Another HR-related use case is that an individual is not seeing their performance plan in the authorized system. Their ticket could include a copy of the performance plan as an attachment. The authorized program area handling the matter can respond/comment within the ticket.

The PII maintained for statistical and research purposes: The data maintained by these IT systems is used for testing and statistical purposes (i.e., Censuses/Surveys) such as resolutions to software issues and to ensure that mandatory survey or statistical information is ready for internal Census Bureau use.

A survey program area related example includes an employee manually entering respondent (members of the public) information into a ticket for defect resolution purposes. When a problem or discrepancy is encountered within an application or database, a tester will create a defect/issue with a full description of what happened during testing along with steps on how to reproduce the reported defect. The testers will communicate by using comment threads until a resolution is reached and the defect is verified/closed.

The description and comment section of a defect should include information regarding the application being executed, and any applicable environment/database/tables being used. In addition, all relevant documentation such as release notes and software specifications, and data input and/or output. If the data input or output, includes any PII or Title 13 data, that information is communicated in a separate email via Kiteworks (email encryption service) or an encrypted message via regular email.

Examples of data may include data entered via the Internet Self Response instrument or data collected using software systems for field data collection operations. Other data inputs may include data that is manually extracted from the OCIO Enterprise Data Lake (EDL).

Document management system:

The PII maintained for information sharing initiatives: Internal Census Bureau teams use the document management system to create, organize, collaborate, and share documentation. This includes projects, plans, meeting notes, and other relevant information. It allows dedicated spaces and pages for projects. Teams can structure information hierarchically,

making it easy to navigate. This system will also be used to provide dashboard metrics and reporting for management. The document management system will be approved for Titled data and PII. Any upload/download of documents is done manually and the capability to block downloads also exists. An example use case for this system would include the use of test and live address data files in support of the 2030 Census; this could also include relevant information about specific addresses.

Source Code Repository:

The PII maintained for administrative purposes: Internal Census Bureau teams use the underlying version control system to help track changes in the source code. Developers can create branches to work on specific features or fixes independently. The system provides project boards to visualize and manage work. They can be customized to fit various project management methodologies. The source code repository system contains very minimal PII such as user ids and name about Census Bureau employees utilizing the systems.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the Census Bureau's/operating unit's use of the information, and controls that the Census 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. 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 PII/Title 13 data.

In addition, the 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 | IPS)
- Firewalls
- Mandatory use of HTTP(S) 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 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 OCIO EDTSB is handled, retained and disposed of in accordance with appropriate federal record schedules.

EDTSB Title data controls have been implemented to meet the data categorization levels.

Section 6: Information Sharing and Access

6.1 Indicate with whom the Census 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 Census Bureau	X		X
DOC Census Bureaus			
Federal agencies			
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 Census Bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC Census Bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC Census Bureau/operating unit before re-dissemination of PII/BII.
X	No, the Census 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.

	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:
X	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	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the ticketing application and collaboration system, the systems do not explicitly ask for PII, PII may reside in the tickets and files uploaded to the collaboration system.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For the ticketing application and collaboration system, the systems do not explicitly ask for PII, PII may reside in the tickets and in files uploaded to the collaboration system. Individuals must consent to particular uses of PII for work related purposes.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For the ticketing application and collaboration system, the systems do not explicitly ask for PII, PII may reside in the tickets and in files uploaded into the collaboration system. There is no opportunity to review/update PII at the EDTSB system level.

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: logs are collected and recorded by the application and reviewed on regular basis
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): _____ X 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.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	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 | 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)
- Encryption of data in transit via Transport Layer Security (TLS)
- 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. 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.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

____ Yes, the PII is searchable by a personal identifier.

_X_ 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
X	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: **GRS 4.2 Item 40**
	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. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X

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.)

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	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: PII collected can be directly used to identify individuals.
X	Quantity of PII	Provide explanation: A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the PII is unlikely to result in limited harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide requirements. Violations may result in serious civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: PII is located on computers controlled by the Census Bureau or on mobile devices or storage media. Access is limited to certain populations of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned equipment outside of the physical locations, and only with a secured connection.
	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 Census 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 Special Sworn Status individuals 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.