Version Number: 01-2019

U.S. Department of Commerce
Office of Financial Management

Privacy Impact Assessment
for the
Commerce Business System (CBS) Solution Center (CSC) Portal

Reviewed by: Maria D. Dumas, 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

Jennifer Goode 08/05/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Commerce Business System (CBS) Solution Center (CSC) Portal

Unique Project Identifier: CSC Portal

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

- CSC Portal is a Minor System; it is a child system of the EAS application system boundary.

(b) System location

- The system is primarily managed by resources located at the CBS Solutions Center in Gaithersburg, MD. The system is physically located at the Federal Aviation Administration Data Center in Oklahoma City, OK.

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

- There are no interconnections to external applications for the systems.

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

- The Office of Financial Management (OFM) Travel Management Division's, Passports and Visas Application has been designed to track the information related to Official and Diplomatic passports, passport applications and visa applications for persons and their spouse, dependents, or otherwise traveling on behalf of the Department of Commerce. The Passports and Visas Application will help make sure that a passport information for an individual on official travel in a known secure location for access if needed during the travel period and that the needs of a traveler's itinerary are met before they travel. This includes the verification that passports and visas have been issued and match the official travel being planned.

- The application is available only to Department of Commerce Travel Management Division (TMD), International Trade Administration (ITA) and National Institute of Standards and Technology (NIST) travel employees with proper access. The information stored in the application is only a subset of the Department of State U.S. PASSPORT RENEWAL APPLICATION for eligible individuals from DS-82. This information is stored for archive retrieval purposes and only provided internal to the Department of Commerce TMD, ITA and NIST travel employees.

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

- Users retrieve the information by accessing the secure website.

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

- Data is entered into the system via the secure website by TMD, ITA and NIST travel employees inputting required information from the DS-82 form. The information will be retained as part of the application. Then the DS-82 is submitted to State Department via courier for normal processing or secure file transfer for expedited processing. Once the passport and visas are issued for the official travel being requested, the information in the application is updated.

(g) Any information sharing conducted by the system

- A traveler's information is quickly available to TMD, ITA and NIST travel employees with proper access.

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

- 22 Code of Federal Regulations 53.1 is the authority that requires the need for a passport when traveling abroad for official duties.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

- CSC Portal is classified as a Moderate system.

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.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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	X	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):Visa information					
*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	X	o. Financial Information	
b. Maiden Name		i. Place of Birth	X	p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender	X	k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
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	X	f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History			
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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		d. Queries Run		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	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email	X		
Other (specify): Emails sent via Secure File Transfer. Fax requests will include an advisory statement about the contents on the cover sheet and the sender will notify the recipient before and after the fax transmission.					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): Data regarding visa number, passport status and validation is provided through either secure email and hard copies from the Department of State. A majority of the information is provided by the traveler.					

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.

A majority of the information in the system is provided by the traveler. Data regarding visa number, passport status and validation is provided through either secure email and hard copies from the Department of State.

Travelers have the ability to review their information and make updates/changes by contacting the TMD, ITA and NIST employees to have changes made within the system in one of the following manners: in person, via secure encrypted email, or hard Copy Mail/Fax. Sending updates by fax is a coordinated effort that requires the sender to contact the recipient in advance. Fax requests will include an advisory statement about the contents on the cover sheet and the sender will notify the recipient before and after the fax transmission.

Any additional information needed such as itinerary, travel approval and Visa information is provided directly by the traveler to the TMD, ITA and NIST Travel Office Employee.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Approval No. 1405-0146
	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).

The Passports and Visas Application has been designed to store the information related to Official and diplomatic passports, passport applications and visa applications for persons and their spouse, dependents, or otherwise traveling on behalf of the Department of Commerce. The passport and visa information will be used to determine if an individual has the appropriate credentials required for official travel and that requirements for traveler's itinerary are met prior to traveling.

The passports and visas information will also be used to make sure that passport information for an individual is always in a secure location and available should it be required for use while individual is on travel. If there is a reason for the information to be accessed while individual is on official travel, TMD, ITA and NIST travel employees will be able to provide the information when needed.

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.)

Some passport data is maintained for at least 15 years, as required by the State Department. Paper documents are maintained until the information has been moved into the application and then shredded afterwards. Also, there is always the potential for insider threat. Annual Cybersecurity Awareness Training is conducted in order to communicate the appropriate procedures for handling/dispensing information.

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
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			
The TMD, ITA and NIST travel employees will populate the application with required information from the DS-82 form. The information will be retained as part of the application. Then the DS-82 is submitted to State Department via courier for normal processing or secure file transfer for expedited processing. Once the passport and visas are issued for the official travel being requested, the information in the application is updated.			

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

6.2 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.

6.3 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.	
	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: .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided to the individual on U.S. PASSPORT RENEWAL APPLICATION FOR ELIGIBLE INDIVIDUALS form DS-82 when he/she completes the form and notice is provided by the TMD,ITA and NIST travel employees when the individual provides his/her information in person.
	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: Individuals must submitting the information to the TMD, ITA and NIST travel employees for official DOC travel. PII/BII is only used for administrative purposes to support DOC Travel.

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: PII/BII is only used for administrative purposes to support DOC Travel.

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: Any Travelers wishing to update/change information must contact the TMD, ITA and NIST travel employee to have changes made within the system in one of the following manners: in person, via secure encrypted email, or hard Copy Mail/Fax. Sending updates by fax is a coordinated effort that requires the sender to contact the recipient in advance. Fax requests will include an advisory statement about the contents on the cover sheet and the sender will notify the recipient before and after the fax transmission.
	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: User access to the Visa/Portal application is reviewed on a semi-annual 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): 8/5/2021 ☐ 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.
X	Other (specify): An MOU/SLA with DOTESC Data Center, where the application is located, is signed and in place. In this SLA, the following breach notification section is in place: Provide reporting of all security incidents for this system in a timely manner to the ESC Data Center's Information Systems Security Officer (ISSO) as well as the DOC ISSO in accordance with ESC Data Center and FAA and DOC/CFO/ASA Incident Response policies. In accordance with DOC security policy, incidents potentially involving Personally Identifiable Information (PII) data shall be reported to the DOC within 45 minutes from initial identification. All other incidents shall be reported to the DOC within one hour from initial identification. Application administrator does not have underlying access to the data. Administrators have access to the supporting servers however, they cannot access the data stored in the database.

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).*

The CSC Portal uses an encrypted web-based front end for data entry to ensure secure transmission of information with a application for storage and retrieval. The Portal creates personalized windows for each user or group of users, based on job functions or roles. Each window or page can bring together information from disparate data sources and provide access to them from a single entry point for TMD, ITA and NIST travel employees with proper access. The CSC Portal is a web portal configured in a two-tier model with the middle-tier components on one physical server and the infrastructure on another with encrypted transmission of information between tiers. The network is configured to allow encrypted internet traffic only from authorized DOC bureau subnets.

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-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons.
	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: DAA-GRS2016-00130001, DAA-GRS2013-00030001 and GRS 5, Item 2
	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	X	Overwriting	
Degaussing		Deleting	X
Other (specify): Some passport data is maintained at least 15 years, as required by the State Department.			

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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The VISA and Passport data can clearly distinguish an individual's identity.
X	Quantity of PII	Provide explanation: The VISA and Passport data will maintain personal information on all Department of Commerce employees and their spouse, dependents, or otherwise involved in official foreign government travel.
X	Data Field Sensitivity	Provide explanation: Visa/Passport Application information contains name, DOB, and passport number which can specifically identify an individual.
X	Context of Use	Provide explanation: PII/BII data contained in Visa/Passport is only used for administrative purposes to support travel for official DOC business. Access to this data is role-based and only available to CSC employees supporting the system, and TMD employees from NIST & NOAA.
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974 (5 USC 552a) and OMB Memorandum M-07-16 to requires the US Government to protect this information.
X	Access to and Location of PII	Provide explanation: Access is to the Visa / Passport application only. Access is limited to CSC personnel as well as TMD, ITA and NIST travel personnel. The servers are located at the Federal Aviation Administration (FAA) Enterprise Service Center in Oklahoma City, Oklahoma. There is a Service Level Agreement (SLA) with the FAA to host the application servers.
	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.)

After a review of the threats associated with the application, it was determined that since this application is primarily used for administrative support, a potential risk of insider threat was noted. To protect against this, each user is provided with annual cyber security training outline how to maintain and access systems with PII. Also role based protections are in place to ensure that users can access data that is only allocated to their

bureau/role/level. Audit logs are captured in the system and retained for after the fact investigations. Audit Logs are reviewed in support of event investigations on an as needed basis.

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.