

**U.S. Department of Commerce  
Office of Financial Management**



**Privacy Threshold Analysis  
for the  
Commerce Business System (CBS) Solution Center (CSC) Portal**

## U.S. Department of Commerce Privacy Threshold Analysis

### Commerce Business System (CBS) Solution Center (CSC) Portal

#### Unique Project Identifier: CSC Portal

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

#### Description of the information system and its purpose:

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) *Whether it is a general support system, major application, or other type of system*
  - CSC Portal is a minor application, and is a child system of the Enterprise Application System (EAS) application system boundary.
- b) *System location*
  - CSC Portal management is located in Gaithersburg, Maryland. Application infrastructure is located at the Department of Transportation – Enterprise Services Center (DOTESC) in Oklahoma City.
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
  - CSC Portal is a child system to the DOC Enterprise Application System.
- d) *The purpose that the system is designed to serve*
  - CSC Portal is a repository for authorized CSC users to share key system documentation.
- e) *The way the system operates to achieve the purpose*
  - CSC Portal 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 Database 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.

- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- The Passports and Visas Database 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.
- g) *Identify individuals who have access to information on the system*
- The CSC Portal database is available only to Department of Commerce Travel Management Division and International Trade Administration travel employees with proper access.
- h) *How information in the system is retrieved by the user*
- Users retrieve the information by accessing the secure database.
- i) *How information is transmitted to and from the system*
- Information is transported into the system via the TMD or ITA travel employees populating the database with required information from the DS-82 form. The information will be retained as part of the database. 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 database is updated.



**Questionnaire:****1. What is the status of this information system?**

\_\_\_\_\_ This is a new information system. *Continue to answer questions and complete certification.*

\_\_\_\_\_ This is an existing information system with changes that create new privacy risks.  
*Complete chart below, continue to answer questions, and complete certification.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

\_\_\_\_\_ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

  X   This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

**2. Is the IT system or its information used to support any activity which may raise privacy concerns?**

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

\_\_\_\_\_ Yes. *Please describe the activities which may raise privacy concerns.*

The VISA and Passport application will collect Visa and Passport numbers including certain demographic data such as date of birth, gender, full name, and job title for Department of Commerce employees who are on official federal travel.

\_\_\_\_\_ No

**3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?**

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption.

"Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

- ☐ Companies
- ☐ Other business entities

☐ No, this IT system does not collect any BII.

#### 4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

☐ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☐ DOC employees
- ☐ Contractors working on behalf of DOC
- ☐ Members of the public (ITA travelers may have spouse and/or dependents traveling with them.)

☐ No, this IT system does not collect any PII.

***If the answer is "yes" to question 4a, please respond to the following questions.***

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

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

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

\_\_\_\_\_ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

\_\_\_\_\_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.***

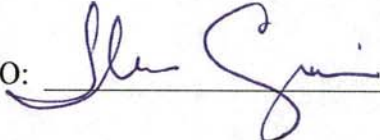


## CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the CSC Portal and as a consequence of this applicability, I will perform and document a PIA for this IT system.

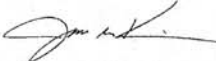
\_\_\_\_\_ I certify the criteria implied by the questions above **do not apply** to the CARTS/Version Manager and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Teresa Coppolino

Signature of SO: 

Date: 4/19/18

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO:  Digitally signed by JUN KIM  
DN: c=US, o=U.S. Government, ou=Department of Commerce,  
ou=Office of the Secretary, cn=JUN KIM,  
0.9.2342.19200300.100.1.1=13001001483988  
Date: 2018.04.23 09:00:29 -04'00'

Date: 4/23/2018

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: 

Date: 4/30/18

Name of Bureau Chief Privacy Officer (BCPO): Kathleen Gioffre

Signature of BCPO: **KATHLEEN GIOFFRE** Digitally signed by KATHLEEN GIOFFRE  
DN: c=US, o=U.S. Government, ou=Department of  
Commerce, ou=Office of the Secretary, cn=KATHLEEN  
GIOFFRE, 0.9.2342.19200300.100.1.1=13001000075444  
Date: 2018.04.24 07:50:33 -04'00'

Date: \_\_\_\_\_