Version Number: 01-2019

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

OFM/Commerce Business System (CBS) Solution Center (CSC) Portal

Unique Project Identifier: CSC Portal is an EAS OS-059 Application

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: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 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.

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

- 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 spouses, 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 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.

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

- Users retrieve the information by accessing the secure application.

i) How information is transmitted to and from the system

- Information is transported into the system via the TMD, ITA and NIST travel employees populating 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.

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.*

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

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

__ __ 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). *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 01-2017 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. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

____ 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.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

____ DOC employees
____ National Institute of Standards and Technology Associates
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

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

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

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

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

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

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

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

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

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

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the 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 CSC Portal 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: TERESA COPPOLINO Digitally signed by TERESA COPPOLINO Date: 2020.02.28 15:11:40 -05'00' Date: _____

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

Signature of ITSO: JUN KIM 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: 2020.03.24 08:19:50 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Lisa Martin

Signature of PAO: LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.05.08 08:13:16 -04'00' Date: _____

Name of Authorizing Official (AO): Stephen Kunze

Signature of AO: STEPHEN KUNZE Digitally signed by STEPHEN KUNZE Date: 2020.03.10 13:19:46 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Maria Dumas

Signature of BCPO: ANGELA WASHINGTON Digitally signed by ANGELA WASHINGTON Date: 2020.05.08 12:25:03 -04'00' for Maria Dumas Date: _____