Version Number: 01-2019

U.S. Department of Commerce
Office of Financial Management (OFM)
Office of Financial Management Systems (OFMS)

Privacy Threshold Analysis
for the
CSC General Support System (GSS) OS-009

U.S. Department of Commerce Privacy Threshold Analysis

Office of Financial Management (OFM)/Office of Financial Management Systems (OFMS)/ CSC General Support System (GSS) OS-009

Unique Project Identifier: 006-03-01-01-01-0510-00

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

The CSC OS-009 is a general support system.

b) System location

The CSC GSS is currently operational at the Department of Commerce (DOC)/Office of Financial Management (OFM)/Office of Financial Management Systems (OFMS)/CBS Solutions Center (CSC), Gaithersburg, Maryland.

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

The CSC GSS OS-009 is a standalone system managed by onsite personnel; however, it interconnects with the DOT/FAA/ESC and HCHB. If an administrator requires server level access to an Enterprise Application Systems (EAS) application, an RDP connection through a VPN is established. The requirements for interconnection between Department of Transportation (DOT), Federal Aviation Administration (FAA) and Enterprise Service Center (ESC) are for providing CBS and EAS applications users located within the CBS Solutions Center (CSC) to access the application services hosted at the DOT/FAA/ESC.

The HCHB VPN connection provides failover service from CBS Solutions Center to FAA.

The CSC does not allow the general public to access to the CSC GSS OS-009.

d) The purpose that the system is designed to serve

.

The CSC provides the information technology infrastructure support to Program Support Division (PSD), which uses PII data to support the Budget Execution/Processing, Strategic Planning, Workforce Planning, Record and Information Management, Acquisitions, Funds Process and onboarding of government and contractors employees.

e) The way the system operates to achieve the purpose

The Primary functions of the CSC GSS OS-009 are to support the Department of Commerce (DOC), Office of the Secretary (OSEC), Office of Financial Management (OFM), Office of Financial Management Systems (OFMS) CBS Solutions Center (CSC) and theTechnical Support Division (TSD) in executing its Enterprise IT Infrastructure, IT Security, Support and Maintenance, Helpdesk Support, Records Retention, IT Logistic Services, System Administration and network support for the OFMS/CSC facility.

The CSC GSS provides technical support to the CBS (OS-051), EAS (OS-059) and DAA (OS-076) applications.

The CSC also provides the information technology infrastructure support to Program Support Division (PSD), which uses PII data to support the Budget Execution/Processing, Strategic Planning, Workforce Planning, Record and Information Management, Acquisitions, Funds Process and onboarding of government and contractors employees.

The CSC GSS provides technical support to the CBS (OS-051), EAS (OS-059) applications which are running at DOT/FAA/ESC in Oklahoma City and have their own PIA's.

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

The CSC GSS OS-009 provides information technology infrastructure support to the CSC government and contractor employees who are involved in developing, testing and maintaining the Commerce Business Systems (CBS), Enterprise Applications Systems (EAS) and Data Act Analytics (DAA) applications that are running in DOT/FAA/ESC Oklahoma city and have their own PIA's.

The CSC GSS OS-009 is collecting, maintaining and using infrastructure to support program support division (PSD).

g) Identify individuals who have access to information on the system

Access to the CSC GSS OS-009 is restricted to DOC Furnished Equipment and only when connected to DOC Networks.

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

Users can download information from various applications based on their assigned user role within the CSC GSS OS-009 system to the shared drives. PSD staff, which uses PII data such as name, address, date of birth, email address, and employee ID number to support budget execution/processing, strategic planning, workforce planning, records management, acquisitions and onboarding of government employees and contractors.

i) How information is transmitted to and from the system

Information is transmitted across approved encryption protocols such as VPN Tunnel, TLS and SFT (secure file transfer).

.

Questionnaire:

1. What is the status of this information system?

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

__X__ 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. _X_ Other changes that create new privacy risks (specify): PII/BII data can potentially be saved on user desktops and on network shared drives.					

____ 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.

____ 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):			

__X__ 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.

__X__ 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."

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

_X___ DOC employees
____ National Institute of Standards and Technology Associates
_X___ 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?

__X__ 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. The CSC Program Support Division (PSD) collects SSN to verify the individual's identity, required for background investigation and for security clearance.
Provide the legal authority which permits the collection of SSNs, including truncated form. 5 U.S.C. 301; 44 U.S.C. 3101; Executive Office (E.O.) 12107, E.O. 131614, 41U.S.C. 433(d); 5 U.S.C. 5379; 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999, DAO 202-430 (performance management system), DAO 205-16 management of electronic records. DAO 210–110; Executive Order 12564; Public Law 100–71, dated July 11, 1987. Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966) 22 Code of Federal Regulations 53.1 is the authority that requires the need for a passport when traveling abroad for official duties. The authority for the maintenance of the system is 28 U.S.C. 3101–3105, Debt Collection Act of 1982 (Pub. L. 97–365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.

____ 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?

_X___ 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.

__X__ 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.