Version Number: 01-2019

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

Privacy Impact Assessment
for the
CSC General Support System (GSS) OS-009

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 07/26/2021

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

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

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

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

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

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) Technical Support

Division (TSD) – Enterprise IT Infrastructure, IT Security, Support and Maintenance, Helpdesk Support, Records Retention, and 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.

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

The CSC users can view and print reports containing only data that is allowed by their role according to the active directory, to their local printers or high-speed printers in their office vicinity. It is the responsibility of the users to handle printed media and supported applications in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of CSC. Users can download information, again based on their assigned user role within the CSC GSS OS-009 system, to the shared drives.

The Program Support Division (PSD) staff, which uses PII data such as Social Security ID, Taxpayer ID, Employee ID, Driver's License ID, Passport, Financial Account, Name, Maiden Name, Gender, Age, Race, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Occupation, Job Title, and Salary to support the Budget Execution/ Processing, Strategic Planning, Workforce Planning, Record and Information Management, Acquisitions, Funds Process and onboarding of government and contractors employees.

(f) 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).

(g) Any information sharing conducted by the system

No information sharing conducted by the CSC General Support System.

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

Includes the following, with all revisions and amendments:

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 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.

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

The CSC OS-009 is categorized as MODERATE.

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): PII 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.

____ 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*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
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: The CSC Program Support Division (PSD) collects SSN to verify the individual's identity, required for background investigation and for security clearance.					

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	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X		
d. Work Telephone Number	X	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	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
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	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

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.

Contractors providing their information as a part of the onboarding process have the opportunity to review and resubmit their information if there are any issues. CSC PSD only stores the information as a part of the onboarding process. Contractors also have the ability to review their information after they submit on OPM e-QIP.

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 No. 1615-0047
	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	
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): b. To automate on-boarding and off-boarding of personnel (government and contractors),			

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 CSC GSS provides support to 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 federal government and contractor employees.

The CSC GSS provides the following infrastructure support to protect the PII data for all the applications at CBS Solutions Center.

- Cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions
- McAfee drive encryption on laptops
- Automatically updates malicious code protection via McAfee Antivirus (AV) and Anti-Spyware for all systems (desktops, servers, including remote access by Laptops)
- Vulnerability scan monthly
- Full backup on all CSC servers every Friday, and the incremental backup is done from Monday thru Thursday. The backup tapes are encrypted and stored at a secured offsite location

- Access Control: access provisioning, access/privileged accounts monitoring
- Security baseline configuration
- Block and filter network traffic and malicious websites
- Secure file transfer - Kiteworks
- PIV card for system access authentication

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.)

There is risk that information in the system could be breached, lost, compromised, or otherwise subject to unauthorized disclosure or exposure by insider threat or other means. To reduce the risk of information or system compromise, the CSC GSS employs appropriate security controls for the system in accordance with NIST 800-53 Rev. 4, as described in Section 8.1 below. Additionally, CSC provides information security awareness training at the point of employee or contractor onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis. Further, users sign an Access and Use policy and Rules of Behavior for access to CSC systems. Finally, the system is subject to regular monitoring by administrators.

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	X	
DOC bureaus	X	X	
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 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.)*

	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: Any form that collects data in support of the EAS Applications provide a Privacy Act statement regarding the collection, use, and dissemination of PII/BII. All administrators at the CSC undergo annual cybersecurity training that includes handling of PII/BII.
	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	Specify why not: CSC GSS OS-009 provides infrastructure.

	opportunity to decline to provide PII/BII.	support to multiple applications that contain PII data. PII/BII must be provided as a condition of employment; In some instances PII/BII must be provided as a requirement to perform certain duties.

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: CSC GSS OS-009 provides infrastructure support to multiple applications that contain PII data. PII/BII must be provided as a condition of employment; In some cases PII/BII must be provided as a requirement to perform duties for employment.

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: For some programs employees can update PII through self-service modules in MYEPP and Human Resource Management System. Contractors can submit PII changes through PSD Staff.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: In some cases PII/BII must be provided as a requirement to perform duties.

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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
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): August 8, 2020 ☐ 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.
	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).*

The CSC network team implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

The CSC network team has employed McAfee drive encryption on laptops.

The CSC network team implements, centrally manages, and automatically updates malicious code protection via McAfee Antivirus (AV) and Anti-Spyware for all systems (desktops, servers, including remote access by Laptops).

The CSC network team scans for vulnerabilities in the information system monthly.

The CSC network team employs monitoring devices IPS and ADAUDIT. The system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

All CSC employees are required to complete Cybersecurity training annually.

All CSC employees are required to sign rules of behavior annually.

A Full backup is performed on all CSC servers every Friday, and the incremental backup is done from Monday thru Thursday. The backup tapes are encrypted.

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/BII 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: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. For the retention of contractor onboarding documentation, CSC follows schedules GRS 2.2 Item 060; Employment Eligibility Verification Records, and GRS 2.1 item 140; Pre-appointment files. For CSC employees that are federal government employees, all onboarding documentation is handled directly by the HCHB Security Office.
	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	X
Degaussing	X	Deleting	X
Other (specify):			

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: Specific individuals are able to be identified.
X	Quantity of PII	Provide explanation: The PII contained in the applications is collected from all Commerce employees and contractors.
X	Data Field Sensitivity	Provide explanation: Data collected contains various PII including SSN.
X	Context of Use	Provide explanation: Data collected contains various PII including SSN for DOC administration.
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974 (USC 552a) and OMB memorandum provide the obligation to the US Government to protect this information.
X	Access to and Location of PII	Provide explanation: PII/BII is only accessed by necessary individuals. The CSC OS-009 servers are located at CBS solutions center, Gaithersburg, Maryland.
	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.)

There is a risk associated with the collection and processing of sensitive information by the system:

Information collected for and maintained within the system includes sensitive PII, including Social Security numbers, Passport, Driver's License, Credit Card and other PII information. As such, the CSC has employed technical and administrative controls for the system in accordance with guidance outlined in NIST 800-53, Revision 4, as well as additional controls for a "Moderate" confidentiality system in accordance with the DOC Privacy Overlay. CSC limits access to the system to a small number of authorized users, approved by Technical Support Division (TSD) director, with specific user roles and system permissions. Administrators regularly monitor the system for misuse.

Regarding data collected for and processed by the system, data points were determined in accordance with Federal standards for conducting background investigations and similar checks related to personnel and physical security. Data points align to Standard Forms used across the government for granting access to information or facilities for employees, contractors, staff, and visitors. Individuals seeking employment with CSC or access to CSC facilities provide data. Opportunities to consent to the collection and use of this Information, and to access, amend and correct such information exist.

The PII application administrators review the number of people who have access to privacy information annually.

There is a risk that user desktop drives are not encrypted. A draft POAM #103287 has been entered into the CSAM. The PSD staff use laptops that have encrypted drives to collect the PII data for the purpose of onboarding staff.

There is also risk of storing PII data on network shared drives, unauthorized employees can potentially access the data. Users and administrators that need to store PII are instructed to store it by encrypting the files and placing it in locations that are not accessible to unauthorized employees. All users who have access to PII data are given training annually on how to store and manage PII data.

The servers are located in a secure room and access is limited to authorized personnel, therefore, to limit the possibility of unauthorized physical modification or damage to the servers.

All CSC employees are required to complete Cybersecurity training annually. The CSC also conducts IT Security day annually where PII training is given to the staff.

All CSC employees are required to sign rules of behavior and Access and User policy annually.

PII files found on the network shared drives are removed and the file owner is reminded of proper handling procedures.

In case unauthorized personnel try to access, modify or delete the PII data file, the CSC network team employs the ADAudit tool, which helps to identify when and who accessed, edited and deleted the file. Nightly backup tapes are encrypted.

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.