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

Privacy Impact Assessment
for the
CARTS/Version Manager

Reviewed by: _____Tahira Murphy_____, 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

_____*Tahira Murphy*_____ 8/24/2022
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer   Date

U.S. Department of Commerce Privacy Impact Assessment
Office of Financial Management/CARTS/Version Manager

Unique Project Identifier: CARTS/Version Manager is an EAS OS-059 Application

<u>Introduction</u>: System Description

Provide a brief description of the information system.

The CBS Application Request Tracking System (CARTS) was developed by Micro Focus Serena Software and is used to track changes to the application code (CBS and CSC/OFM Portal) as well as changes to Documentation, network and hardware configurations for the Commerce Solution Center (CSC).

The application is used by Bureau users, CBS software developers and testers, CSC Software Configuration Management team, functional leads and managers. Changes are tracked in CARTS via AR (Activity Request) tickets, SR (Service Request) tickets, and/or CR (Change Request) tickets.

PVCS Serena Version Manager is a Software Configuration Management (SCM) tool, which stores the core CFS, CPCS, Data Warehouse, CCR, and TIBCO application code. It is used by the CBS software developers, testers, and CSC Software Configuration Management team to track application code changes and maintain proper version control of all the application code. There is traceability to CARTS ARs each time any software is updated by the development team. The SCM Team labels all software with a unique Release Number in Version Manager when software deliveries are performed.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
- CARTS/Version Manager (VM) is a Minor System; it is a child system of the Enterprise Application System (EAS) application system boundary.

(b) System location
- CARTS/VM is physically located at Department of Transportation Enterprise Services Center (DOTESC) 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 connections to external applications for the systems

(d) The way the system operates to achieve the purpose(s) identified in Section 4
- The CBS Application Request Tracking System (CARTS) was developed by Micro Focus Serena Software and is used to track changes to the application code (CBS and

CSC/OFM Portal) as well as changes to Documentation, network and hardware configurations for the Commerce Solution Center (CSC). The application is used by Bureau users, CBS software developers and testers, CSC Software Configuration Management team, functional leads and managers. Changes are tracked in CARTS via AR (Activity Request) tickets, SR (Service Request) tickets, and/or CR (Change Request) tickets.

- PVCS Serena Version Manager is a Software Configuration Management (SCM) tool, which stores the core CFS, CPCS, Data Warehouse, CCR, and TIBCO application code. It is used by the CBS software developers, testers, and CSC Software Configuration Management team to track application code changes and maintain proper version control of all the application code. There is traceability to CARTS ARs each time any software is updated by the development team. The SCM Team labels all software with a unique Release Number in Version Manager when software deliveries are performed.

(e) How information in the system is retrieved by the user
- A typical transaction in CARTS involves a user logging in with their user ID and password from their desktop. Once they have accessed the application, the user can then manage the tickets related to their job function. This includes but is not limited to submitting new requests, updating the status of existing tickets, and closing requests once they have been completed. Users can search for both active and closed tickets but can only view those that are associated with their role.

(f) How information is transmitted to and from the system
- Over the DOC network, to DOC workstations. CBS Solutions Center in Gaithersburg, MD has a network path, which carries traffic from and to our desktops through HCHB to DOTESC Data Center in Oklahoma City. Firewall rules are in place to allow connections to servers on specified ports.

(g) Any information sharing
- There is no information sharing conducted by the system. CARTS is only available to approved DoC users. Employees with a business need are added to the system as a part of the initial roll-on process.

(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

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
- CARTS/VM are part of the Enterprise Applications Systems (EAS) OS-059. CARTS/VM 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):					

____ 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.

_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.

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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		f. 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		Hard Copy: Mail/Fax		Online	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
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.

> The request is approved by their immediate supervisor & approved by a member of the CSC management team.

2.4   Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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 is 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 about a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The DOC-assigned phone number and email address are entered prior to the provisioning of an account so that the administrator can notify the user once the account is ready to use. Once the account is active a user can see the contact information of the POC's associated with their tickets. Users also receive system-generated email updates regarding their tickets any time the status is changed. All PII collected is referenced to federal employees and contractors.

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 not any known PII data stored in the applications. The BII information stored contains server names in the applications, as part of the daily work performed. Collectively with information from other DOC servers, the information stored in CARTS & Version Manager, could provide enough evidence to create a picture of how DOC is structured and operated. As such the information could be sensitive in nature.

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 PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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.

6.4 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: _____.	
	Yes, notice is provided by other means.	Specify how:
X	No, notice is not provided.	Specify why not: It has been determined that CARTS/ Version Manager is not a system of records.

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: The information is required in order to notify a user once their account has been created, as well as to facilitate the management of tickets.

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: Users are notified that their PII is used only for the limited purposes of account provisioning and request management.

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: Users can view their account profile and make their own updates if needed.
	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: Access to the PII/BII is restricted to those roles that require the information to support them job functionality.
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): 8/7/2021 ☐ 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.
X	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).*

CARTS is not a public facing system and can only be accessed from a DOC network as an authenticated user. The servers are located at DOTESC where CARTS resides, and are maintained by administrators that configure the servers to be in a secure state as part of the service level agreement (SLA) between DOC and DOTESC. In addition, servers are physically secured in a room requiring specific personnel access, to limit the possibility of unauthorized physical modification or damage. In addition, servers are in a physically secure room with access by specific designated personnel, to limit the possibility of unauthorized physical modification or damage.

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: General Records Schedule (GRS) 3.1, Item 30
	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.)*

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII collected is not searchable by a personal identifier and is already accessible through a search on public Commerce websites.
X	Quantity of PII	Provide explanation: PII is collected for Commerce employees and support contractors who have a business need to access

		CARTS, and only their government-issued email and phone number are recorded.
X	Data Field Sensitivity	Provide explanation: The PII that is collected for CARTS is already accessible through a search on public Commerce websites.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	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.)

No potential threats to privacy were discovered. However, there is always the potential for insider threat. DOC requires the annual Cybersecurity and Privacy Awareness training for all employees, which will help mitigate this threat.

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.

Points of Contact and Signatures

Information Technology Security Officer	**Chief Information Security Officer**
Name: Eduardo Macalanda Office: DOC OFMS Phone: 301-355-5987 Email: emacalanda@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: EDUARDO MACALANDA Date signed: _____ Digitally signed by EDUARDO MACALANDA Date: 2022.08.16 14:46:50 -04'00'	Name: Densmore Bartly Office: OS OCIO Phone: 202-482-3186 Email: dbartley@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DENSMORE BARTLY Date signed: _____ Digitally signed by DENSMORE BARTLY Date: 2022.08.19 15:29:01 -04'00'
System Owner	**Authorizing Official**
Name: Teresa Coppolino Office: DOC OFMS Phone: 301-355-5501 Email: tcoppolino@doc.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: TERESA COPPOLINO Date signed: _____ Digitally signed by TERESA COPPOLINO Date: 2022.08.18 08:15:56 -04'00'	Name: Zachary Schwartz Office: DOC OS CIO Phone: 202-577-1769 Email: zschwartz@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ZACHARY SCHWARTZ Date signed: _____ Digitally signed by ZACHARY SCHWARTZ Date: 2022.08.20 09:33:54 -04'00'
Authorizing Official	**Privacy Act Officer**
Name: Stephen M. Kunze Office: Office of Financial Management Phone: 202-482-3709 Email: skunze@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: STEPHEN KUNZE Date signed: _____ Digitally signed by STEPHEN KUNZE Date: 2022.08.18 15:02:13 -04'00'	Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Tahira Murphy Date signed: _____ Digitally signed by Tahira Murphy Date: 2022.08.24 21:50:26 -04'00'
Section intentionally left blank.	**Bureau Chief Privacy Officer** Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Tahira Murphy Date signed: _____ Digitally signed by Tahira Murphy Date: 2022.08.24 21:51:02 -04'00'

13

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page <u>must</u> be removed prior to publication of the PIA.