Version Number: 01-2019

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

Privacy Threshold Analysis
for
CARTS/Version Manager

Office of Financial Management/CARTS /Version Manager

Unique Project Identifier: CARTS/Version Manager 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:

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

- 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 purpose that the system is designed to serve

- 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) The way the system operates to achieve the purpose

- CARTS/VM is a hierarchical representation of a group of projects, subprojects, and versioned files. CARTS/VM is not a relational database; instead, CARTS/VM stores the configuration settings for an entire collection of projects, subprojects, and versioned files.

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

- PII (government issued phone number and government issued email address) is collected from Employees and Contractors for the sole purpose of initial account administration and help desk services. All PII is self-reported and is no different from the employee information on publically accessible Commerce websites

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

- CARTS is used by the EAS/CBS software developers, testers, CBS Solution Center (CSC) Software Configuration Management team, functional leads and managers. CARTS is also accessible to DOC users located at HCHB.
- Version Manager is used by the EAS/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.

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

- Using a GUI application connecting to the application server. 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 have the ability to search for both active and closed tickets, but can only view those that are associated with their role.

i) How information is transmitted to and from the system

- Information is transmitted across approved encryption protocols such as HTTPS, SSH, and SFTP. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 180-1, and Secure Hash Standard issued by NIST when necessary.

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 CARTS/VM 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/VM 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 15:09:53 -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 08:12:53 -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 08:32:46 -04'00' Date: _____

Name of Authorizing Official (AO): Stephen Kunze

Signature of AO: STEPHEN KUNZE Digitally signed by STEPHEN KUNZE Date: 2020.03.10 13:18:54 -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 09:44:48 -04'00' for Maria Dumas Date: _____