

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



**Privacy Threshold Analysis
for the
CARTS/Version Manager**

U.S. Department of Commerce Privacy Threshold Analysis

Office of Financial Management/CARTS /Version Manager

Unique Project Identifier: CARTS/Version Manager

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*
 - CARTS is the change management application currently used to create and track AR (Activity Request) tickets, SR (Service Request) tickets, and CR (Change Request) tickets. There is a custom workflow solution implemented for the ARs, SRs and CRs. CARTS was created using Solutions Business Manager Software application. CARTS is used by software developers, testers, Software Configuration Management teams, functional leads and managers to track changes to the application code, documentation plus network and hardware configurations for the CSC.
 - PVCS Version Manager (VM) is a Software Configuration Management (SCM) tool, which stores the "core" CFS, CPCS, Data Warehouse, CCR, and TIBCO application code. The software developers, testers, and CSC Software Configuration Management team to track application code changes and maintain proper version control of all the application code use it. There is traceability to

CARTS Activity Requests 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.
- 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 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. *Please describe the activities which may raise privacy concerns.*

☐ 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 about: *(Check all that apply.)*

☐ Companies

☐ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

☐ DOC employees

☐ Contractors working on behalf of DOC

☐ 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 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.

- 4c. 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, and/or 4c 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.

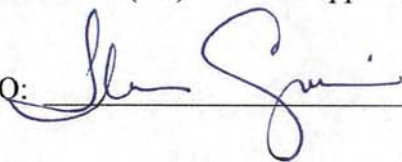
CERTIFICATION

 X I certify the criteria implied by one or more of the questions above **apply** to the CARTS/Version Manager 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/Version Manager 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: _____

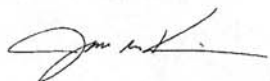


Date: _____

4/19/18

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

Signature of ITSO: _____



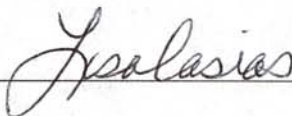
Digitally signed by JUN KIM
DN: c=US, o=U.S. Government, ou=Department of
Commerce, ou=Office of the Secretary, cn=JUN
KIM, 0.9.2342.19200300.100.1.1=13001001483988
Date: 2018.04.23 08:46:49 -04'00'

Date: _____

4/23/2018

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: _____



Date: _____

4/30/18

Name of Bureau Chief Privacy Officer (BCPO): Kathleen Gioffre

Signature of BCPO: _____

KATHLEEN GIOFFRE

Digitally signed by KATHLEEN GIOFFRE
DN: c=US, o=U.S. Government, ou=Department of
Commerce, ou=Office of the Secretary, cn=KATHLEEN
GIOFFRE, 0.9.2342.19200300.100.1.1=13001000075444
Date: 2018.04.24 07:40:04 -04'00'

Date: _____

