Version Number: 01-2019

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Personal Property Management System (PPMS)

U.S. Department of Commerce Privacy Threshold Analysis

Office of Administrative Programs/Personal Property Management System (PPMS)

Unique Project Identifier: PPMS 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: *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

- PPMS is a Minor System; it is a child system of the EAS application system boundary.

(b) System location

- The system is primarily managed by resources located at the CBS Solutions Center in Gaithersburg, MD. The system is physically located at the Federal Aviation Administration Data Center (DOT/FAA/ESC) 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)

- PPMS has an interconnection with WEX Inc. GSS for the purpose of transmitting unidirectional data communication between these entities. PPMS accesses encrypted data within WEX, and retrieves data on a daily schedule.

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

- Personal Property Management System (PPMS) provides Department of Commerce (DOC) with a mechanism to ensure uniformity within and across the agency in the selection and management of personal property. PPMS provide the critical information that DOC decision-makers require to purchase, transfer, dispose/excess, and depreciate personal property. Sunflower Systems offer an integrated software suite that provides property managers the ability to monitor, control and account for all property transactions. Sunflower's mobile solutions for receiving, physical

inventory, shipping, and excess management simplify property processes by bringing asset data to a handheld device. Sunflower Assets System controls asset management tasks by managing physical and financial accountability in a single web-based system. Portable scanners are utilized in international offices in order to allow a user to modify an asset. The scanners connect to the user's desktop which allows them to access the record associated with a piece of property. The user then enters the information into the database. The DOC has implemented a Fleet Management Information System to manage its fleet of approximately 3,000 vehicles worldwide. The majority of vehicles are already entered in DOC's Sunflower Personal Property Management System (PPMS), to track them as personal property assets. DOC also owns the Sunflower Federal Automotive Statistical Tool (FAST) Solution. Sunflowers standard functionality coupled with the FAST Solution provides the Department with the necessary software components to implement a Fleet Management Solution.

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

- Users are able to account for and manage their assets from the time of acquisition through disposal. A complete history is maintained as records are easily updated to reflect any changes (location, user, value, etc.). Users may also generate reports to view assets. Once assets are disposed and a final event is created, a history of the assets remain in the system for reporting purposes in the future.

(f) How information is transmitted to and from the system

- Data is transferred into the DOC enclave and assimilated to the PPMS Development, Test, and Production environments. For the reports from CitiBank, a direct connection is made each month to a CitiBank database server. The reports are then pulled into the PPMS environments from the database server. These files are transferred via SFTP using a Secure Shell (SSH) tunnel encrypted with an RSA token.

(g) Any information sharing conducted by the system

- In support of the Fleet implementation, PPMS requires files from two external entities. On a daily basis, reports are delivered to PPMS from CitiBank. On a monthly basis, reports are delivered to PPMS form the General Services Administration (GSA) inventory. For the GSA reports, the reports are delivered to an external facing server at the Department of Transportation / Federal Aviation Administration / Enterprise Services Center (DOT/FAA/ESC) over Secure File Transfer Protocol (SFTP). The files are then brought through the DOT/FAA/ESC external firewall to an internal server over File Transfer Protocol (FTP).

(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; E.O. 12107, E.O. 13164, 41 U.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 210–110; Executive Order 12564; Public Law 100–71, dated July 11, 1987.

- The Consolidated Omnibus Budget Reconciliation Act of 1986, Sections 15301 and 15302 require federal executive agencies (Pub. L. No. 99-272) (40 U.S.C. Sec. 17502 and 17503) to have a centralized system to identify, collect, and analyze motor vehicle data with respect to all costs incurred for the operation, maintenance, acquisition, and disposition of motor vehicles. To help mitigate deficiencies, respond to significant deficiencies noted in the OIG Audit dated September 2010, and comply with GSA Bulletin FMR B-15 and Presidential Memorandum on Federal Fleet Performance, dated May 24, 2011

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

- PPMS is classified as a Moderate system.

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 PPMS 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 [IT SYSTEM NAME] 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 or SO: TERESA COPPOLINO Digitally signed by TERESA COPPOLINO Date: 2020.02.28 15:13:49 -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 08:28:04 -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 09:06:48 -04'00' Date: _____

Name of Authorizing Official (AO): Stephen Kunze

Signature of AO: STEPHEN KUNZE Digitally signed by STEPHEN KUNZE Date: 2020.03.10 13:21:27 -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 12:19:13 -04'00' for Maria Dumas Date: _____