# U.S. Department of Commerce
# Office of Administrative Programs

## 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: OS015 – OAS General Support System – Sunflower (PPMS)**

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

b) *System location*
    - The PPMS management office is located in Washington, DC. Application infrastructure is located at the Department of Transportation – Enterprise Services Center (DOTESC) in Oklahoma City.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
    - PPMS is a child system to the DOC Enterprise Application System.

d) *The purpose that the system is designed to serve*
    - 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.

e) *The way the system operates to achieve the purpose*
    - PPMS offer an integrated software suite that provides property managers the ability to monitor, control and account for all property transactions. The 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.

f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
   - PPMS collects transactional information from federal employees and contractors/associates in connection with their working relationship with BEA, BIS, Census, EDA, ESA, ITA, MBDA, NIST, NOAA, NTIA, and NTISs.

g) *Identify individuals who have access to information on the system*
   - Access to PPMS information is granted to authorized DOC users responsible for ensuring uniformity within and across the agency in the selection and management of personal property.

h) *How information in the system is retrieved by the user*
   - PPMS information is accessed through the integrated software suite.

i) *How information is transmitted to and from the system*
   - User information is transferred securely from the bureaus to PPMS for accurate user and account administration.

**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.*

_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 01-2015 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 PPMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of System Owner (SO): Teresa Coppolino

Signature of SO: ________________ Date: 3/7/19

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: 2019.03.11 14:34:29 -04'00' Date: __________

Name of Authorizing Official (AO): Stephen Kunze

Signature of AO: ________________ Date: 4/12/19

Name of Bureau Chief Privacy Officer (BCPO): Wes Fravel

Signature of BCPO: WESLEY FRAVEL Digitally signed by WESLEY FRAVEL
Date: 2019.04.16 15:23:01 -04'00' Date: __________