Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Personal Property Management System (PPMS)

Reviewed by: Kathleen Gioffre, Office of the Secretary (OS) Privacy Officer

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: 2017.07.19 09:13:50 -04'00'

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.07.26 15:16:30 -04'00' 7/18/2017

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of Administrative Programs/ Personal Property Management System (PPMS)

Unique Project Identifier: An Enterprise Application System (EAS) OS-059 Application

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

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. 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. The Privacy Impact Assessment covers the Personal Property Management System (PPMS).

(b) a description of a typical transaction conducted on the system

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.

(c) 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 J.P. Morgan Chase & Co. (JMPC). 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). The data is transferred into the DOC enclave and assimilated to the PPMS Development, Test, and Production environments. For the reports from JMPC, a direct connection is made each month to a JPMC database server. The reports are then pulled into the PPMS environments from the database server. These files are transferred via SFTP using an Secure Shell (SSH) tunnel encrypted with an RSA token.

(d) a citation of the legal authority to collect PII and/or BII

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

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

PPMS is an application within the EAS OS-059 environment which 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.

_X___ This is an existing information system in which changes do not 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):					

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*		e. File/Case ID		i. Credit Card	X
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	X
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): GOV or CTR, office room/cube #, JBID, supervisor information, organization code number, and location of assets					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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	X	d. 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			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	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 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 are 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			
To determine eligibility		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 in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The PII identified in Section 2.1 is in reference to federal employees and contractors/associates in connection with their working relationship with BEA, BIS, Census, EDA, ESA, ITA, MBDA, NIST, NOAA, NTIA, and NTISs. The data will be used for purposes of providing access to delivering better services, and for carrying out of property and asset management activities. User information will be transferred securely from the bureaus to PPMS for more accurate user and account administration.

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 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	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: Census: BOC CBS, Single Sign On NIST: Webservice, Single Sign On, SFTP NOAA: LDAP, & Staff Directory All systems are fully assessed and authorized to operate by Authorizing Officials at the respective bureaus.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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.)*

X	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:
	No, notice is not provided.	Specify why not:

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: It is required under Property Bulletin #005, FY10# for import of BII information.

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: It is required under Property Bulletin #005, FY10# for import of BII information.

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: Individuals have an opportunity to review the PII/BII information via the annual inventory process.
	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.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	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: User access roles are reviewed on a quarterly basis.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/11/2016 ☐ 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 (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
X	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.

The user administration data that is transferred to PPMS is sent as an XML file over SFTP. Unauthorized use of the system is restricted by user authentication. PPMS is not a public facing system and can only be accessed from a DOC network as an authenticated user. Access logs are kept and reviewed for any anomalies. The servers are located at DOT/ESC/FAA where PPMS 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 DOT/ESC/FAA. In addition, servers are in a physically secure room by specific personnel access, to limit the possibility of unauthorized physical modification or damage.

Section 9: Privacy Act

9.1 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Employees Personnel Files Not Covered by Notices of Other Agencies-COMMERCE/DEPT–18. http://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html Property Accountability Files -SORN COMMERCE/DEPT-16. http://osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-16.html

	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 Schedules (GRS) 20, Item 3
	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		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

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

X	Identifiability	Provide explanation: Information regarding users only includes the information in regards to their status as a Commerce employee. A Majority of the information can be found publically

		online using the Commerce Employee Directory
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: Information regarding users only includes the information in regards to their status as a Commerce employee. A Majority of the information can be found publically online using the Commerce Employee Directory
X	Context of Use	Provide explanation: Information used to ease administration and authentication of PPMS users
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.