Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary / Office of Financial Management

Privacy Impact Assessment
Office of Financial (OFM) Data Analytics Program
For the Procurement, Development and Testing Life Cycle Stages

Reviewed by: Kathy 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: 2018.02.16 15:03:02 -05'00'

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

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.03.06 12:50:54 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Office of Financial Management / Data Analytics Program

Unique Project Identifier:

Introduction: System Description

The OFM is initiating a data analytics program with the objective of developing the capability to identify trends, anomalies and other meaningful patterns in financial programs. This program will analyze data from three Department of Commerce (DOC) programs: purchase card transactions, travel card transactions and payroll (mainly time and attendance). The system will utilize data from the system of records for the time and attendance record keeping (WebTA), payroll management (NFC), purchase and travel card transactions system (PaymentNet). Although this Privacy Impact Assessment (PIA) broadly describes the entire program, Senior Agency Official for Privacy approval is limited to the procurement, development and testing life cycle stages.

The OFM data analytics program will involve the development of continuous monitoring processes for sensitive programs. The monitoring process will include several steps to request, transform and load data into existing databases where analytical tests will be applied to assist in identifying trends, anomalies and other meaningful pattern in the data.

Data processing for the program includes data calls to the WebTA database administrator, who will utilize scripts that have been provided by the program developers to extract the requested data; a request for data will also be sent to the NFC database administrator and the administrator for the PaymentNet database. Once the extracts are received, tests are performed to verify the completeness of each data set. Integrity tests include comparing employee headcount between the two systems.

The OFM staff and contractors will have access to the data being tested. The OFM contractors will build and run the initial tests, OFM staff will review for instances where controls may have been compromised and/or circumvented.

Tests run against the data include stratifications for payroll pay types such as; regular and premium pay types sorted by; bureau, pay time, employee and date. Additionally, tests are performed to look for and identify instances where controls have been compromised and/or circumvented, examples for payroll include, unapproved leave and/or premium pay, self-certification of timesheets, inappropriate use of federal holidays, night and Sunday differential. Compromised purchase and travel card controls are identified using a risk-ranking process to review each transaction and cardholder. Risk rankings include but are not limited to: adult entertainment, duplicative payment-same vendor, non-zero sales tax, split payment-same employee, transaction over purchase limit, potential conflict of interest, and potentially personal transaction.

The testing results are compiled and presented to Department and Bureau management on a case-by-case basis. The purpose of presenting these results is to determine the areas that require additional

review and follow-up. If needed, Departmental and Bureau management will prepare and maintain corrective action plans designed to prevent future breakdowns in controls.

System of Records and the Legal Authority for maintenance of the systems:

Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309.

Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

31 U.S.C. 3321 and 40 U.S.C. 486(c)

Based on Federal Information Processing Standards Publication; Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199).

The overall security categorization level for the system is **MODERATE**. Security Category Impacts for the OFM Data Analytic Program:

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.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X	g. New Interagency Uses	X
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

The initial procurement, development and testing life cycle stages of this program will not use any live data. The information identified below reflects the data intended for use when the program is fully implemented, However, these data elements are subject to change as the program progresses through the life-cycle stages.

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	X
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintains, or disseminates 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	X	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		g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): *Employee grade, position, pay plan and organization code*					

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): **N/A**					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify): *Contractors entering into an agreement for services with the Department shall be contractually subject to all Department of Commerce and Federal IT Security standards, policies, and reporting requirements. The contractor shall meet and comply with all Department IT Security Policies and applicable Department and NIST standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.*

Including but not limited to the following:

- *access control*
- *security awareness*
- *audit and accountability*
- *identification and authentication*
- *incident response*
- *system maintenance*
- *media protection*
- *physical and environmental*
- *system and information integrity*
- *system and communication protection*
- *key management*

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): *Not a source system*					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): *The source for each data element will be coming from OS and other DOC bureaus.* • *PaymentNet – purchase and travel card transactions for DOC employees* • *WebTA – time and attendance activity for DOC employees* • *NFC – payroll information for DOC employees*					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): *N/A*					

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): *To identify weaknesses and strengthen existing internal controls weaknesses. Aid Department and Bureau management decision making by identifying, anomalies, patterns and trends.*			

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 OFM data analytics program will receive PII data from existing systems of records; WebTA, NFC and PaymentNET using FIPS compliance data transfer.

Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and information Systems", is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security related areas. Contractor systems supporting the Department must meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 4, DOC IT Security Program Policy, Commerce Information Technology Requirements (CITRs) and Policy Memos, which provide DOC specific implementation parameters and details.

The results of the data analytics are then analyzed and compiled for presentation to Department of Commerce management on a case-by-case basis. A continuous monitoring function is anticipated for the program, where previously collected data are maintained and combined with current data as part of the analytic process.

Information described in section 2.1 relates to Department of Commerce purchase and travel card holders and the related vendors. Purchase and travel card holders are exclusively DOC employees.

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 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: *The IT system for this program is yet to be identified. However, the contract is dependent on the vendor system being FISMA and FedRAMP(if applicable) compliant. The Department of Commerce, OCIO will review the technical controls and no data will be transferred to, or processed by the system prior to the granting of an ATO.*
	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. Purpose of access is to allow for the testing and analysis of data as described in the introduction and statement of work for this project. *(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: _____.	
X	Yes, notice is provided by other means.	Specify how: Under initial collection for the following systems: WebTA, NFC, PaymentNet
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Under initial collection for the following systems; WebTA, NFC, PaymentNet
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Under initial collection for the following systems: WebTA, NFC, PaymentNet
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: *Data has been previously collected by the system of record. Individuals will not have access to the data or reports and will not be able to make adjustments. Individuals can continue to make changes to their PII in the original systems of record.*

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	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: *PII/BII data will reside on the contractor system which has been issued an authority to operate, meeting the security criteria required by DOC OCIO. The contractor system has been reviewed by DOC OCIO and is required to undergo annual assessments and reviews to maintain the ATO issued by DOC OCIO.*
X	The information is secured in accordance with FISMA requirements. *The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Accreditation (A&A). NIST Special Publication 800-37 Rev 1 gives guidelines for performing the A&A process. The contractor system/application must have a valid assessment and accreditation (signed off by the Federal government) before going into operation and processing Department information.* *A&As are conducted at the outset of procuring/implementing/entering into an agreement to use a service that will process, store, or transmit DOC info. Systems and/or services are then monitored pursuant to an agreed upon continuous monitoring plan, and the system or service receives an affirmation of an authorization to operate (ATO) on at least an annual basis as long as the continuous monitoring plan is implemented as agreed and the risks to the system/service remain within thresholds acceptable to the DOC Authorization Official (AO) for the system/service.* *The system must have a new A&A conducted (and signed off on by the Federal government) at least every three (3) years or at the discretion of the Authorizing Official when there is a significant change to the system's security posture. All NIST 800-53, Revision 4 controls must be tested/assessed no less than every 3 years. DOC Risk Management Framework CITR-19 contains requirement for continuous monitoring.* *As the Department finalizes the procurement process for this project an A&A will be conducted and and ATO granted.* ☒ This is a contractor owned system.
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.
X	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.

• *Contractor system with an ATO provided by DOC OCIO* • *Data to be transmitted to and from contractor using DOC secure file transmission technology.*

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)*: • COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; • COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons; and • COMMERCE/DEPT-22, Small Purchase Records.
	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, Transmittal 24 (Aug 2015), National Archives Office of the Chief Records Officer, section 1.1 1.1 Financial Management and Reporting Records*
	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		Overwriting	
Degaussing		Deleting	X
Other (specify): *As specified in the record control schedule*			

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. *Per FIPS 199 review*
	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	*The information directly identifies a large number of individuals using names, addresses and financial information.*
X	Quantity of PII	*The information directly identifies several thousand individuals and organizations.*
X	Data Field Sensitivity	*The information includes addresses, salary, position descriptions and individual financial account information, if accessed inappropriately could potentially lead to identity theft. Additionally, certain fields when combined may highlight potentially sensitive relationships.*
X	Context of Use	*Statistical analysis will be performed on the data collected from each system.*
	Obligation to Protect Confidentiality	
X	Access to and Location of PII	*PII included in the results of processing may be transferred offsite on a case-by-case basis to DOC bureaus not located in HCHB. Files are transmitted using the approved DOC secure file transfer processing*
	Other:	

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.