Version Number: 01-2019

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

Privacy Threshold Analysis
for the
OFM Data Analytics Program

U.S. Department of Commerce Privacy Threshold Analysis

Office of Financial Management / Data Analytics Program

Unique Project Identifier:

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

The Office of Financial Management Data Analytics Program is a Major Application (MA), hosted on servers within the existing Department of Commerce (DOC or "Department) Office of Information Technology Services General Support System (OITS-GSS) boundary, (OS-064)[1].

b) System location

The OFM Data Analytics Program is hosted on a server located within the Herbert Clark Hoover Building (HCHB), located at 1401 Constitution Avenue, NW, Washington, DC.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The OFM Data Analytics Program consists of two dedicated servers within the OITS-GSS, on which a suite of analytic tools and capabilities exist. The servers receive regular, non-automated (manual) data ingests from existing systems to include:

- ***WebTA***[2]: The Department's time and attendance tracking system;

[1] For purposes of this PIA, the terms OITS-GSS and OS-064 are used interchangeably.

[2] The Privacy Impact Assessment for the WebTA solution is available at: http://www.osec.doc.gov/opog/privacy/OS%20PIAs/OS-059_WebTA_and_Archive_Time_PIA_SAOP_Approved.pdf

- ***CitiManager***: The application currently used by the Department to manage its purchase and travel card program. CitiManager replaces the PaymentNET program described in the prior PIA;
- ***E-Gov Travel Service 2 System (ETS2)***[3]: ETS2 is a web-based, end-t-end travel management system to plan, authorize, arrange, process, and manage official federal travel. ETS2 is owned and operated by the General Services Administration (GSA). The system enables travelers and/or travel arrangers to plan and make reservations (air, rail, lodging, car rental, etc.) on-line, prepare travel authorizations and vouchers on-line, and produce itineraries, have tickets issued, and store receipts on-line. ETS2 serves as the Department's end-to-end travel authorization and voucher system;
- ***The National Finance Center's (NFC) Personnel/Payroll Database (PPS):*** The NFC is a Shared Service Center under the Office of Personnel Management (OPM) Human Resources Line of Business. The U.S. Department of Agriculture (USDA) relies on its information technology systems, including the PPS, to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, like DOC, and the public at large. The PPS consists of personnel and payroll data and is used by the DOC for personnel and payroll processing.

For all the systems outlined above, data will be uploaded manually using DOC approved transfer protocols (secure email, e.g. Kiteworks) and methods.

d) The purpose that the system is designed to serve

The Office of Financial Management (OFM) is implementing a "Data Analytics Program" with the objective of identifying trends, anomalies and other meaningful patterns across DOC programs – focusing on financial systems. This program will analyze data from three DOC areas: Purchase card transactions, travel (to included travel card transactions), and payroll. As outlined above, the system will rely on data from existing DOC systems, as well as systems operated primarily by other Federal agencies where DOC is a customer (NFC, ETS2). OFM staff and select OFM contractors will have access to the data being tested. OFM contractors will build and run the initial tests. OFM staff will review for instances where controls may have been compromised and/or circumvented. The Data Analytics Program will be rolled out in three phases – Pilot Phase, Phase I, and Phase II. While each is described below, the primary focus of this PIA is Phase I. The OFM Data Analytics Program is also addressed at a high level in the OS-064 PIA.

[3] The Privacy Impact Assessment for the ETS2 solution is available at: https://www.gsa.gov/cdnstatic/E2-Solutions%20TAVS%20PIA%20webversion%20signed%20January%2011,%202018.pdf

e) The way the system operates to achieve the purpose

Pilot Phase

In 2015, OFM conducted a study to determine the feasibility of implementing a data analytics program. The conclusion of the feasibility study recommended implementing a pilot program using three programs to determine the scale of potential control weaknesses or other anomalies. OFM engaged a contractor to perform the pilot program. The contractor utilized their in-house IT systems and provided industry proven analytic tools and services to perform the pilot data analytics program. This pilot program was reviewed, approved, with certain restrictions, by the DOC Senior Agency Official for Privacy (SOAP). The OFM Data Analytics pilot program was documented in a previous version of this PIA and, at a high level, in the OS-064 PIA which is the system on which data is maintained and manipulated. Based on the pilot program, OFM decision makers decided to move forward with the implementation of a permanent data analytics program.

Phase I

Phase I of the permanent OFM Data Analytics Program includes the collection and processing of data from existing DOC systems, including PII, to facilitate development of continuous monitoring processes for sensitive financial programs across the Department. The monitoring process will include several steps to request, transform and load data into existing databases and analysis, housed on servers within the OS-064 environment, where analytical tests will be applied to assist in identifying trends, anomalies and other meaningful pattern in the data. These tools include traditional Microsoft tools like Excel and Access, as well as more advanced tools and analytics capabilities like Tableau, "R" and SQL server.

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 similar request for data will be sent to the NFC PPS database administrator and the administrator for the PaymentNet (now CitiManager). Data extracted from ETS2 will be limited to existing "canned" reporting capabilities. 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.

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 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 results of this data analysis 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.

It is important to note that the results of the analytics are used to strengthen weaknesses in controls related to financial programs only. The intent is not to target or reprimand any specific individual, employee, or groups of employees or individuals.

Phase II (Future State)

As noted above, the OFM Data Analytics Program will be rolled out in phases. The first phase, a Pilot Phase, was addressed in a previous version of this PIA. Phase I – as addressed in this PIA – formalizes the OFM Data Analytics Program as a permanent, regularly occurring process involving the intake and processing of PII from the systems outlined above, as well as the acquisition of contract support to facilitate data processing efforts and make recommendations for long-term implementation of a robust data analytics program. In conducting the pilot phase, OFM determined that due to the unique IT system requirements and specialized tools and capabilities required to implement a robust data analytics program, the use of a contractor and their in-house systems is a key component of a successful data analytic program within OFM. Thus, OFM will be looking to eventually – in Phase II – acquire a specific set of tools and technologies, along with continued contractual support to build out the program. These updates will be covered in updates to this PIA.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

Information analyzed will include purchase card transactions, travel card transactions, and payroll (mainly time and attendance), including PII associated with specific employees for each of these information types, such as credit card (travel and purchase) account numbers, employee IDs, employee names, as well as work related data such as job title, work address and email address, and salary information. As noted above, the primary purpose of the program is the identification of breakdowns in controls related to financial programs through data analytics – the results of the analytics are used to strengthen weaknesses in controls related to financial programs only. The intent is not to target or reprimand any specific individual, employee, or groups of employees or individuals.

g) Identify individuals who have access to information on the system

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. As necessary, Department and Bureau management may be presented with aggregate analytical results in the form of reports, which are used to address breakdowns in financial program controls.

h) How information in the system is retrieved by the user

Information is retrieved in the form of reports about specific topics of interest to the OFM Data Analytics Program as outlined above. While not the intent, this could include retrieving by specific employees (name or employee ID) in relation to payroll records or travel or purchase card purchases. Generally, data will be retrieved by querying against combined datasets for patterns of non-compliance with existing internal DOC controls. For example, inappropriate use of certain pay types, or unauthorized transactions against a purchase card.

i) How information is transmitted to and from the system

Data is transmitted to the system via data calls to the WebTA, NFC PPS, and CitiManager database administrators, who will utilize scripts that have been provided by the program developers to extract the requested data. Data extracted from ETS2 will be limited to that which is available in existing, "canned" reporting capabilities in the web interface

Data is transmitted from the system in the form of reports, on a case-by-case basis as requested by Departmental and Bureau management and developed through existing reporting tools via secure email transmission (Kiteworks) to the designated point of contact for upload and capabilities such as Tableau.

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		f. Commercial Sources		i. Alteration in Character	

Management Changes				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):			

_X__ 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.

_X__ 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."

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

__X_ DOC employees
____ National Institute of Standards and Technology Associates
__X_ 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.

_X__ 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?

_X__ 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.

_X__ 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 the OFM Data Analytics program 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 Information System Security Officer (ISSO) or System Owner (SO): Julie Tao

Signature of ISSO or SO: HAIFAN TAO Digitally signed by HAIFAN TAO Date: 2020.07.16 11:54:31 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jerome Nash

Signature of ITSO: JEROME NASH Digitally signed by JEROME NASH Date: 2020.07.15 13:44:02 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Lisa J. Martin

Signature of PAO: LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.09.28 17:26:50 -04'00' Date: _____

Name of Authorizing Official (AO): Larry Anderson

Signature of AO: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2020.09.04 14:45:48 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Maria Dumas

Signature of BCPO: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2020.09.28 22:59:47 -04'00' Date: _____