Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
For
OFM Data Analytics

U.S. Department of Commerce Privacy Threshold Analysis

OFM Data Analytics

Unique Project Identifier: [TBD]

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 of the information system and its purpose in a way that a non-technical person can understand.* 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).

The Office of Financial Management (OFM) is currently implementing a data analytics program with the objective of developing the capability to identify trends, anomalies and other meaningful patterns in financial programs. Phase I of the OFM data analytics program was initiated as a pilot project to analyze data from three Department of Commerce (DOC) programs; purchase card transactions, travel card transactions and payroll (mainly time and attendance).

The results of the pilot process analytic process were reviewed and presented to Department management for further review and follow-up.

Phase II of the implementation of the OFM data analytics program will involve the development of continuous monitoring processes for sensitive programs, the conversion of existing management metric reports and performing additional ad hoc data analytics. The continuous monitoring process will build off previous analytics in order to be able to better identify trends and patterns.

OFM will be utilizing a vendor operated system to process and store data related to this program. The vendor system will meet DOC IT security requirements.

The program will extract and analyze data from multiple sources. Time and attendance data will be pulled from the WebTA system and joined with data from the NFC payroll system. Purchase card and Travel card data will be extracted from the PaymentNet system. If needed, data will be extracted from CBS and Momentum, the Department's accounting and finance systems.

Questionnaire:

1. What is the status of this information system?

_X__ 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. *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.

_X__ Yes. *Please describe the activities which may raise privacy concerns.*

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

____ 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

__X__□ 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..."

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

_X__ DOC employees (data from NFC, WebTA, PaymentNet and possibly CBS and Momentum)
____□ 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?

__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.

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.

_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, 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 OFM Data Analytics 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 OFM Data Analytics and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer (ISSO) or System Owner (SO): **Julie Tao**

Signature of ISSO or SO: ________________ Date: 4/6/17

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: 2017.04.18 10:17:12 -04'00' Date: 4/18/2017

Authorizing Official (AO): **Gordon Alston**

Signature of AO: ________________ Date: 4/7/17

Bureau Chief Privacy Officer (BCPO): **Michael J. Toland, Ph.D.**

Signature of BCPO: MICHAEL TOLAND Digitally signed by MICHAEL TOLAND
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=MICHAEL TOLAND, 0.9.2342.19200300.100.1.1=13001000249566
Date: 2017.05.05 15:45:24 -04'00' Date: 5/5/17