Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
OFM Data Analytics Program

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

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

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

Lisa Martin for Dr. Jennifer Goode 11/18/2021

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

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) 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;
- **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-to-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

[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 [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

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 way the system operates to achieve the purpose(s) identified in Section 4

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.

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.

As noted above, this PIA is focused on phase I. The program remains in phase I, due to the complexities of developing multiple analytics and a temporary restriction in resources due to the continuing pandemic.

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.

(e) 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.

(f) 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.

(g) Any information sharing conducted by the system

Sharing is limited to internal Department and Bureau Management. In some cases, findings may be requested as part of a Congressional, Inspector General, or similar request, and will be provided, as appropriate and in accordance with DOC policies. The system has no direct outbound sharing connections.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Authority for the OFM Data Analytics Program is outlined in:

- Title 5 U.S.C.
- Title 31 U.S.C. 66a, 492

- Title 44 U.S.C. 3101, 3309
- 31 U.S.C. 3321
- 40 U.S.C. 486(c)
- Budget and Accounting Act of 1921
- Federal Claim Collection Act of 1966
- Accounting and Auditing Act of 1950

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

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. *(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):					

____ 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.

____ 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 01-2017).

__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 01-2019 or later).

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

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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		f. Queries Run	X	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): • CitiManager – purchase and travel card transactions for DOC employees • WebTA – time and attendance for DOC employees • ETS2 – business travel records for DOC employees • NFC PPS – payroll information for DOC employees					

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

2.3 Describe how the accuracy of the information in the system is ensured.

Information required by WebTA is provided by the employee during start of employment. Users can review and update their information when gaining access to WebTA. E2 users can review all documents and update their information through the bureau and departments travel office. Department travel and purchase card holders provide their account information when applying for Citibank accounts.

OFM does not and will not verify the accuracy of the files maintained in the system or the contents therein. Information is verified for accuracy and currency at the time of collection, creation, or by mechanisms specific to source system from which it is derived. Data within these source systems is obtained from DOC bureaus, offices, and agency officials and, as such, the originating DOC bureau or office providing the information for each system is responsible for ensuring the accuracy of information included in each source system.

That said, OFM has developed quality control processes as well as utilizes industry best practices during the extract, transformation, and load of data to ensure the accuracy and completeness of the data received and processed.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program		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, and to 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 data containing PII from existing DOC systems, to include: WebTA and CitiManager, as well as the NFC's PPS database. Data as described in Section 2.1 of this PIA relates to current and former DOC employees. References to financial information are DOC purchase and travel card holders and any related vendors.

Specifically, the following data types are acquired from each source system:

- WebTA: Data includes employee name(s), days and hours worked (time and attendance), leave requests and approval records, leave usage records (sick, annual,etc.), supervisor name, title/position, business contact information (email address office location, phone number);
- CitiManager: Data includes name(s), account numbers, employee ID's, title, business contact information (email address, phone number), personal contact information (if provided) to include email address and home address, and transaction records (e.g. purchase records), to include date, type of purchase, vendor information, and amount.-
- NFC PPS: Data includes employee names, employee ID, pay and similar financial records including wages and salary, deductions, merit awards, etc. While the NFC PPS contains extensive PII such as Social Security number, Date of Birth (DOB), bank and routing information, etc., such information is not included in data calls from OFM to the PPS administrator for the purposes of the Data Analytics program.
- ETS2: Data includes names of DOC employees who have traveled, information about specific trips taken including reason, limited information on accommodations, flights, and cost breakdowns per trip, as well as position and supervisor information. Limited business contact information such as email address and phone number are also included in the ETS2 system but are not available in the canned reporting used by OFM for the Data Analytics Program.

OFM acquires data from each system through various means. Data from the ETS2 and CitiManager systems is acquired by downloading files from each system. OFM receives NFC data via download. Data from WebTA is provided via a data call from OFM to the DOC database administrator for each WebTA instance.

Data is analyzed and compiled for presentation to DOC management on a case-by-case basis on a range of topics, such as a lack of appropriate approvals, excessive expenditures, duplicate payments and identifying areas where controls may need to be strengthened. 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. As noted above, the results of the analytics are used to identify and strengthen weaknesses in controls related to financial programs. The intent is not to target or reprimand any specific employee(s).

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is a risk of insider threat. To mitigate the risk of this and other threats, the system has assigned roles for each user, as well as processes and procedures in place to manage access and system permissions. OFM determines and sets the roles according to the user's needs.

All DOC users (employees and contractors) are subject to signing and abiding by an Access and Use policy (i.e. a "Rules of Behavior") for access to and use of DOC systems and the information processed on them. Signing the Access and Use policy is a precondition for being granted access to DOC IT systems and users must also take mandatory cyber security training, which includes detailed training regarding deterring, detecting and reporting incidents of insider threats, prior to being granted access to IT systems. Further, users must take annual refresher training to maintain access to IT systems. Additionally, DOC uses software to monitor system and server event logs for malicious or unusual activity. Finally, DOC has implemented a Data Loss Protection program to identify potentially unauthorized or unsecured disclosures of sensitive PII.

There is risk that information in the system could be breached, lost, compromised, or otherwise subject to unauthorized disclosure or exposure: To reduce the risk of information or system compromise, DOC employs appropriate security controls for the system in accordance with NIST 800-53, as described in Section 8.1 below. Additionally, DOC provides information security awareness training at the point of employee onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis. Further, users sign an Access and Use policy (i.e. a "Rules of Behavior") for access to DOC systems. Finally, the system is subject to regular monitoring by administrators as described above.

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): In some cases, findings may be requested as part of a Congressional, Inspector General, or similar request.	X		

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: The OFM Data Analytics Program is hosted on servers housed within the existing OITS-GSS (OS-064). This server, and the OS-064 GSS, are owned and managed by DOC ES. The system is FISMA compliant, with an ATO, issued on 10/16/2018, and last authorized on 2/14/2020, and subject to an annual review of select controls. The system receives data, in the form of manual uploads, from the following DOC operated systems: - CitiManager – purchase and travel card transactions for DOC employees. - WebTA – time and attendance activity for DOC employees. Additionally, the system receives data, in the form of manual uploads from the following non-DOC operated systems:

	- U.S. Department of Agriculture's (USDA) National Finance Center (NFC) database, Payroll/Personnel System (PPS). o PPS is owned and operated by the NFC on behalf of DOC (and other agencies) and is used to manage and process payroll for DOC employees. Information in the system includes information regarding national ID (SSN), job data, compensation data, location information, etc. Data selected by OFM will not include SSNs. - General Service Administration's (GSA) E-Government Travel System 2 (ETS2). o ETS2 is owned and operated by the GSA on behalf of DOC (and other agencies) and provides an end-to-end travel authorization and voucher system for employees required to travel as part of their duties. For U.S. Department of Agriculture's (USDA) National Finance Center (NFC) database, Payroll/Personnel System (PPS) and General Service Administration's (GSA) E-Government Travel System 2 (ETS2): The SQL Server Integration Services (SSIS) Data Tool is used to import into the Data Analytics database, data files that have been received from source systems and saved to the OS in-house server. The OS virtual servers and the OFM SQL-Server are both DOC in-house servers. Data from the following systems is received by secure file transmission. - For the PPS, WebTA, upon receipt a data call from OFM Data Analytics Program, the database administrators for each system will use scripts provided by the program to extract the requested data and transfer it, via secure email transmission (Kiteworks) to the designated point of contact within the OFM Data Analytics Program for upload and analysis. - For Citi Manager and ETS2, data extracts will be limited to those "canned", pre-determined reports available through each system's web application, which may only be accessed by authorized users via a DOC network.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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: _____.

X	Yes, notice is provided by other means.	Specify how: Users are provided notification at the original point of collection under the following systems: WebTA, NFC PPS, CitiManager and ETS2. The PIA's for each of these systems, as well as the System of Record Notices outline collectin and use of this data. Additionally, for each source system, Privacy Act Statements are provided at the original point of collection on various forms (paper and electronic) on which information is collected for that system.
	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: While individuals may decline to provide PII for original source systems from which data is derived, they may not decline its use within the OFM Data Analytics Program. Individuals who decline to provide information for source systems may not be eligible for employment with DOC and thus, their information would not be included in the OFM Data Analytics Program. As noted above, the intention of the program is not to identify or take actions on specific individual employees.

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: Individuals do not have opportunities to consent to particular uses of their PII, including sharing such information with the OFM Data Analytics Program. In providing their PII for original source systems from which data is derived, individuals are consenting to use of their data by the Data Analytics Program. As noted above, the intention of the program is not to identify or take actions on specific individual employees.

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 source system. Individuals will not have access to the data or reports in the Data Analytics Program and will not be able to make adjustments. Individuals can continue to make changes to their PII in the source system, in accordance with the System of Records under which the source system operates.

		As noted above, the intention of the program is not to identify or take actions on specific individual employees.

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: Explanation: For Phase I of the project, PII/BII data will reside on dedicated servers within the OS-064 environment. The system has been reviewed by DOC OCIO and is required to undergo annual assessments as part of the overall assessment of the OS-064 environment.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 7/3/2021 ☐ 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 (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC ownership rights over data including PII/BII.
	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. *(Include data encryption in transit and/or at rest, if applicable).*

As noted above, the OFM Data Analytics Program is a Major Application housed on the OITS-GSS (OS-064). As such, the servers which house data for the OFM Data Analytics program, and all applications which process related data inherit a multitude of layered security controls from the OITS-GSS to protect PII at rest, during processing, as well as in- transit. These NTST 800-53 controls, at a minimum, are deployed and managed at the enterprise level and include, but are not limited to the following:

- Intrusion Detection and Prevention Systems (TDS TPS)
- Firewalls
- Use of trusted internet connection (TIC)
- Anti-virus software to protect host/end-user systems
- HSPD-12 compliant PIV cards
- Access controls

The OITS-GSS systems also follow the National Institute of Standards and Technology (NTST) standards, including special publications 800-53, 800-63, 800-37, etc. DOC systems which contain, transmit, or process BII/PII, including the OITS-GSS, has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended.

Additionally, DOC provides information security awareness training at the point of employee onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis.

Contractors entering into an agreement for services with the Department, including those supporting the OFM Data Analytics Program are contractually subject to all DOC and Federal IT Security standards, policies, and reporting requirements. Contractor access is limited to contractor staff who have signed non-disclosure agreements and are assigned to the project.

Finally, the system is subject to regular monitoring by administrators via various tools employed within DOC. Included in these are a Data Loss Prevention (DLP) capability which monitors traffic for unauthorized or unsecured disclosures of sensitive PII. Only authorized OFM personnel have access to PII. Data is maintained and encrypted at rest on the system.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(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 COMMERCE/DEPT-22, Small Purchase Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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 Schedule (GRS) 1.1: Financial Management and Reporting Records, July 2017.
	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	X
Degaussing		Deleting	X
Other (specify):			

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

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

X	Identifiability	Provide explanation: PII includes direct identifiers, such as full names or unique identifying numbers (ID).
X	Quantity of PII	Provide explanation: Includes records or more than 10,000 unique individuals.
X	Data Field Sensitivity	Provide explanation: Includes, that if lost, comprised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual or the Department. The information, which includes addresses, salary, position descriptions and individual financial account information, if accessed inappropriately could potentially lead to identify theft. Additionally, certain fields when combined may

		identify relationships, which could have detrimental effects for individuals and the Department.
X	Context of Use	Provide explanation: Information is not used in making determinations about specific individuals' rights, benefits, or privileges. Statistical analysis will be performed on the data collected from each source system.
X	Obligation to Protect Confidentiality	Provide explanation: Explicit promises of confidentiality regarding the information have been conveyed to the subject individuals at the time or point of collection, and other information is protected from unauthorized disclosure by statute or regulations (the Privacy Act of 1974).
X	Access to and Location of PII	Provide explanation: PII is maintained and stored primarily locally, and access is limited to OFM employees and select contractors with a bona-fide need-to-know, the results of processing may be transferred on a case-by-case basis to DOC bureaus not located in HCHB. Files are transmitted using the approved DOC secure file transfer protocol (secure email, e.g., Kiteworks).
	Other:	

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There is a risk associated with the collection and processing of sensitive information by the system:
Information collected for and maintained within the system includes sensitive PII. Insider threat is also a considered risk. As such, the DOC has employed technical and administrative controls for the system in accordance with guidance outlined in NIST 800- 53, Revision 4, as well as additional controls for a "High" PII confidentiality system in accordance with the DOC Privacy Overlay. DOC limits access to the system to a small number of authorized users, approved by OFM, with specific user roles and system permissions. The system is regularly monitored for misuse by administrators.

Regarding data collected for and processed by the system, the data collected was determined based on tests planned to return the greatest value with the least amount of sensitive data. In some cases, source systems limit the amount of PII included or available for extract from the system. In other cases, OFM worked directly with the system administrators to limit the amount of PII or specific, sensitive data points, to reduce risk. For example, OFM did not deem Social Security numbers (SSNs) necessary to link WebTA data to NFC PPS data. OFM worked around the issue by developing alternate methods of linking transactions to the NFC PPS database utilizing existing fields and sophisticated data analytic techniques.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Explanation: Guidelines and operating procedures are being developed by OFM and contract support to reduce the risk posed by comingling potentially sensitive PII from disparate systems. Further, OFM worked directly with CSC business partners to limit its access to/collection of PII from travel records to existing non-sensitive canned reports as outlined in this PIA.
	No, the conduct of this PIA does not result in any required business process changes.

12.3 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.