U.S. Department of Commerce
Office of the Chief Information Officer
Office of the Secretary

Privacy Impact Assessment
Office of Information Technology Services General Support System (OS064)

WESLEY FRAVEL

Digitally signed by WESLEY FRAVEL
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=WESLEY FRAVEL, 0.9.2342.19200300.100.1.1=13001003618524
Date: 2018.09.17 09:39:48 -04'00'

Reviewed by: ________________________________, 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

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: 2018.09.28 18:44:51 -04'00'

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

Office of Information Technology Services-General Support System (OS064)

Introduction: System Description

Web Application Services: The Department of Commerce Office of Information Technology Services General Support System (OITS-GSS) security impact category is moderate. Web Applications is a component of the OITS-GSS.

The Department of Commerce (DOC) and its operating units use various websites and applications, such as commerce.gov, open.commerce.gov and ESA.gov, to engage in dialogue, share information, and collaborate with the public. These sites contain official information from the DOC; they are the authoritative source of official Department information. The DOC owns these websites and applications. These websites and applications continue to grow in size and diversity.

These websites and applications are used to collaborate and share information online by facilitating public dialogue, providing information about or from the DOC, make information and services more widely available, and to improve customer service. Our use of these websites and applications offer important opportunities for promoting the goals of transparency, public participation, and collaboration. Through these services, individuals or groups can create, organize, edit, comment on, combine, and share content of mutual interest.

The Department and its operating units use internal websites and applications to interact with one another, share information, and collaborate. The internal websites are only accessible to Department personnel. Department personnel information, business information and documentation is shared on these internal websites.

The system collects name, day and month of birth, education, general work-related data, and photographs of Department personnel, as well as standard system administration/logging data. This information will be stored on the OITS-GSS. Department personnel biographies will be shared with the public and Department personnel. The PII collected by this system will not be monitored or destroyed until the system is decommissioned. Records will be retained and disposed of in accordance with applicable records schedules.

Typical transactions

a) Media where official DOC users may have an account to use applications tailored to the specific website.

b) Video and image websites where official DOC users may have an account to post videos and images. Public users do not need an account to submit comments.

c) Blogs and similar websites where official DOC users may have an account to post.

d) On internal websites, biographical pages about Department personnel are updated to share information with other personnel. On external websites, biographical pages about Department personnel are updated to share information with the public.

e) Work related information and documentation are posted on internal websites to be accessed by Department personnel.

Authorities supporting the DOC's use of websites and applications:

a) 5 U.S.C. § 301, The Federal Records Act

b) The President's Memorandum on Transparency and Open Government, January 21, 2009

c) The OMB Director's Open Government Directive Memorandum, December 8, 2009

d) OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010

File and Printer Services: The Department of Commerce (DOC) Office of Information Technology Services General Support System (OITS-GSS) provides enterprise applications, local area network (LAN) services, network management and office automation services. The OITS-GSS is located at the Herbert Clark Hoover Building (HCHB) located at 1401 Constitution Avenue, Northwest, Washington, DC.

Programs, Typical Transactions, Information Sharing and Legal Authorities

Twenty-three (23) Business Operating Units (BOU) within DOC use OITS-GSS services for data storage and retrieval of program information supporting official daily responsibilities and the organization's mission. Information use is limited to: developing policies, managing programs and providing oversight for collaborative efforts with business customers. The official needs of the BOU determine the extent of the information sharing with other organizations. The organization restricts and controls the use of all personally identifiable information (PII) and business identifiable information (BII); an individual's job roles and responsibilities determine accessibility within each respective program office. The following BOUs are users of these services:

Office of the Secretary:

1) **Office of Business Liaison (OBL)**

Typical transaction

As part of the OBL's responsibilities, the names and contact information for key individuals from the private sector and relevant industry associations are collected, stored in excel files on internal shared drives and, as appropriate, shared internally with other officially relevant DOC bureaus. The business processes also include compiling the data on spreadsheets and using the information to extend invitations to relevant events hosted by the DOC and/or to arrange one-on-

one meetings with members of the team. Collection and use of this data are critical to the OBL's official mission of representing private sector interests through strategic engagement.

Information sharing

Information is shared within OBL internally and with other officially relevant DOC bureaus.

Legal authority to collect

The authority for maintenance of the systems includes the following sources with revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 131614; 41 U.S.C. 433(d); Executive Order (E.O) 11625; DOO 25-4A and 15 U.S.C. § 1512.

2) Center for Faith Based and Neighborhood Partnerships (CFBNP)

Typical transaction

The collection of PII is for submission for meetings and events on behalf of Commerce employees. CFBNP collects Web Automatic Verification of Enrollment System security information for meetings at the White House conducted with external stakeholders and/or Commerce staff.

Information sharing

The CFBNP shares information with the White House Liaison Office and essential White House staff members to obtain entry clearance for authorization to attend meetings on the White House premises.

Legal authority to collect

The authority for maintenance of the systems includes the following sources with revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 13164; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; Department Administrative Order 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

3) Office of Acquisition Management (OAM)

Typical transaction

A typical transaction involving BII is one in which Civil Applicant System (CAS) receives proposals in response to published solicitations. Depending required method to receive these documents (e.g., postal mail, electronic or hand-delivery, some BII may be received through the CAS. If the information is received by CAS, OAM prints and maintains copies in the contract file; the electronic files received in the CAS are archived in an e-mail folder maintained by the contracting officer/specialist.

Information sharing

As necessary, information is shared between the Office of Inspector General, the Legal Office, Policy Office and the Office of Small and Disadvantaged Business Utilization when solicitation protests require legal review and potential action.

Legal authority to collect

The legal authorities to collect BII include: DOO 20-26 and the Federal Acquisition Regulation (FAR) 9.104-1. According to FAR 9.104-1, there are a number of actions the contractor/vendor must prove to the government in order to be considered as a prospective contractor.

4) Office of Facilities and Environmental Quality (OFEQ)

Typical transaction

A typical transaction involving non-sensitive PII is one in which a user account is created with a user name and an e-mail. The email is used by the system to send automated email notifications of pending required corrective actions that are based upon a previously conducted environmental assessment. The user name is used to create logon ability to the system's environmental databases; these databases consist of two types: 1) existing federal and state environmental regulations and 2) the individual facility assessment results.

Information sharing

OFEQ does not disseminate PII/BII information on the OITS-GSS.

Legal authority to collect

Compliance with all environmental laws and regulations is required by Executive Order 12088.

5) Office of Budget (OB)

Typical transaction

The OB does not have a routine requirement to collect PII. However, OB occasionally collects PII from DOC personnel attending OB meetings at the New Executive Office Building. This pre-clearance information is required by the Office of Management and Budget (OMB) for building access.

Information sharing

The PII collected for the includes: name, city/ state of residence, date of birth, social security number and country of birth. This information is transmitted to OMB using the DOC/OCIO

Accellion Secure File Sharing service.

Legal authority to collect

The authority for OB is derived from 15 USC §1501. Establishment of Department; Secretary; seal – There shall be at the seat of government an executive department to be known as the Department of Commerce, and a Secretary of Commerce, who shall be the head thereof, who shall be appointed by the President, by and with the advice and consent of the Senate, and whose term and tenure of office shall be like that of the heads of the other executive departments; and the provisions of title 4 of the Revised Statutes, including all amendments thereto, shall be applicable to said department. The said Secretary shall cause a seal of office to be made for the said department of such device as the President shall approve, and judicial notice shall be taken of the said seal.

6) Office of Civil Rights (OCR)

Typical transaction

Typical transactions would include events as a part of formal complaints describing actions and the dates of these actions. Transactions of this information would include: assignment of an investigator, hearing requested by complainant and agency's decision issuance.

Information sharing

Information is shared between Office of Civil Rights (OCR) and the Equal Employment Opportunity (EEO) Offices at the National Institute of Standards and Technology (NIST), National Oceanic and Atmospheric Administration (NOAA) and the U.S. Census Bureau (Census) based on customized, role-based levels of bureau and user access. For example, OCR users can access data entered by Census EEO staff and some OCR users can edit that data for official business. Census EEO staff can access data entered by OCR, but access is limited to Census cases and OCR entries are read-only for Census staff.

Legal authority to collect

The authority for processing discrimination complaints within the DOC has been delegated to the OCR Director IAW DOO 20-10, Office of Civil Rights. The DOC's internal discrimination complaint program is described by DAO 215-9.

The authority for the Department's EEO complaint processing program is contained in the regulations of the Equal Employment Opportunity Commission (EEOC) at 29 CFR § 1614 and policy guidance provided by EEOC Management Directive 110. Related laws and regulations governing DOC's authority to process complaints of discrimination include: 42 U.S.C. 2000e-16; 29 U.S.C. 633a; 29 U.S.C. 791 and 794a; 29 U.S.C. 206(d); E.O. 10577; 3 CFR 218 (1954-1958 Comp.); E.O. 11222, 3 CFR 306 (1964-1965 Comp.); E.O. 11478, 3 CFR 133 (1969 Comp.); E.O. 12106, 44 FR 1053 (1978) and Reorganization Plan No. 1 of 1978, 43 FR 19807 (1978).

7) Office of Financial Management (OFM)

Four distinct OFM programs use OITS-GSS services for data storage and retrieval of program information to support official daily responsibilities: Passport/Visa Access Database, Travel Card Program, Sunflower Personal Property Management System and OFM Data Analytics.

Example 1:
Typical transaction

Passport/Visa Access Database is used to track and maintain official and diplomatic passports and visas for various bureau Federal employees, their spouses, and dependents traveling with a Department of Commerce (DOC) employee. This database is an internal system accessed only by the Travel Management Staff. The passports, visas, and applications are tracked to and from various embassies and the Department of State. A typical transaction would be to enter the employee's information into the database and extract various reports. Traveler Information includes: full names, email address, Bureau, Department, title, relationship to DOC traveler, name(s) of spouse and/or dependents traveling with DOC employee, Dates (separation, departure, reviewed, granted, issuance, expiration, employee notification, hold information, cancelation instructions and return address. Visa Application Information includes: Passport number, Embassy name (location and dates - returned, approved, sent to Embassy), application status, picked up (date and by whom), Visa/Passport holder notification date.

Information sharing

The information in the database is not shared – only Travel Management Staff have access to the database.

Legal authorities to collect

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

Example 2:
Typical transaction

JP Morgan Chase System is used to manage the Travel Card Program. A typical transaction conducted in the system is to check for delinquent accounts and extract various reports.

Information sharing

The information is shared - Department Level 1 Agency/Organization Program Coordinator

(A/OPC) has access to the entire system, Bureau Levels 2 & 3 A/OPCs have access to only their travelers' information, and Travel Card holders have access to their account information only. Information is transmitted through an encrypted application process.

Legal authority to collect

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

Example 3:
Typical transaction

Sunflower Personal Property Management System is used to maintain accountability of all personal property assets and fleet of vehicles across the Department. A typical transaction conducted in the system is to enter traveler information, visa information, and extract reports.

Information sharing

The information is shared within DOC with all Bureau Property Officials including those in the field offices and the Sunflower Contractor.

Legal authorities to collect

5 U.S.C. 301, 44 U.S.C. 3101, 40 U.S.C. 481-92, and 15 U.S.C. 1518.

Example 4:
Typical transaction

OFM Data Analytics – The 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. This program will analyze data from three DOC programs: purchase card transactions, travel card transactions and payroll (mainly time and attendance). The system will use data from the system of records for the time and attendance record keeping (WebTA), payroll management (NFC), purchase and travel card transactions system (PaymentNet).

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 use 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.

Tests run against the data include stratifications for payroll day 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.

Information sources

The source for each data element comes from OS and other DOC bureaus.

a) PaymentNet – purchase and travel card transactions for DOC employees.

b) WebTA – time and attendance activity for DOC employees.

c) NFC – payroll information for DOC employees.

Information sharing

OFM staff and OFM contractors will have access to the data. OFM contractors will run the initial tests, as identified in the statement of work for the applicable contract. OFM staff will review for instances where controls have been compromised and/or circumvented. The testing results are compiled and presented to DOC 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.

Legal authorities to collect

Title 5 U.S.C.; Title 31 U.S.C. 66a, 492; Title 44 U.S.C. 3101, 3309; 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; Federal Claim Collection Act of 1966; 31 U.S.C. 3321 and 40 U.S.C.

486(c).

8) Office of Human Resource Management (OHRM)

Typical transaction

The OHRM uses a wide variety of the Department's Human Resources Information Technology (HRIT) systems to provide Department-wide human resources services. The typical transactions are loaded into HRIT systems via online entry into web-based forms by Human Resource (HR) personnel. Bulk transfers of information occur from DOC to Office of Personnel Management (OPM) and U.S. Department of Agriculture (USDA) National Finance Center (NFC) via approved and tested electronic interfaces. These interfaces have approved information interconnection agreements. The OHRM has full responsibility for the design and development of the following IT systems to support HR programs:

a) Automated Classification System (ACS) – ACS contains key position data that supervisors use to create and simultaneously classify Demonstration Project position descriptions. In addition to creating new position descriptions, the ACS stores descriptions in a local user database and allows the user to create a new description based on one in the database; to revise, review, print, or delete position descriptions; or to review and report on the position descriptions in the database.

b) Performance Payout System (PPS) – PPS provides the functionality to record, document and report the annual employee performance rating, performance increase, and bonus payout, calculate the annual comparability increase (ACI) for the employees who are under the Commerce Alternative Personnel System (CAPS) pay plans and transmit updated data to the U.S. Department of Agriculture's National Finance Center (NFC), the Department's Payroll System of Record.

c) Executive Resources Information System (ERIS) – End of Year - Senior Executive Service (SES) Bonus Pool (BP) – SES BP provides the functionality to record and report the annual performance ratings, performance increases, and bonus recommendations, calculate ACIs for the SES employees, and transmit the updated data to NFC.

d) DOC-Hiring Management System (DOC-HMS) – HMS tracks and reports on the timeliness of the 80-day hiring process, and hiring actions initiated by the DOC's Human Resources Operations Center (DOCHROC), as part of the overall human resources management measurement project. This system tracks all the hiring steps from the job announcement to the day a new employee reports for duty. It tracks each step of the process and produces the necessary reports to measure the process effectiveness and efficiency.

e) Honor Awards Nominee System (HANS) – HANS is an automated Gold and Silver Honor Awards Program nomination and reporting system. This system provides users access to nominate employees and vote on nominations, and produce reports including certificate citations, program booklets, and seating charts.

f) WebTA – WebTA is Kronos Proprietary software. It is used to record DOC employees' time and attendance data. The employees enter their own time and attendance data. The data is transmitted bi-weekly to NFC for employees pay processing.

g) Executive Resources Information System-Top Level (ERIS-TL) – ERIS-TL provides information regarding the incumbency status of all key positions to a limited cadre of the most senior Department of Commerce (DOC) executives to aid in Executive Level (SES) Staffing decisions.

Information sharing

Information is shared within Commerce Bureau/Operating Units (BOU) on a case by case basis. Information is shared with OPM and NFC via bulk transfer.

Legal authority to collect

The authority to deliver, maintain and approve Department-wide and approve bureau-specific automated human resources systems and serve as the focal point for collection and reporting of human resources information within the Department of Commerce is delegated to the Office of Human Resources Management in DOO 20-8 - SECTION 4, the Office of Human Resources Management.

The authority for maintenance of the systems includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 131614; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; E.O. 12554, P.L. 100-71, dated July 11, 1987, and Office of Financial Management (OFM) Page 62.

9) Office of Privacy and Open Government (OPOG)

OPOG collects PII as part of the normal duties. The information may contain a variety of sensitive and non-sensitive. The amount of and type would be based on the type of program transaction and submission manner. The information is collected from federal employees, contractors, non-government personnel, and foreign nationals.

Example 1:
Typical transaction

The typical OPOG transaction would be the following: Freedom of Information Act (FOIA)/Privacy Act (PA) transactions include the requester's name, home or business address, personal or business email address, home or business telephone number, and a description of the requested records. FOIA requests are logged into a FOIA tracking system, FOIAonline; see separate DOC FOIAonline Privacy Impact Assessment for more details.

PA transactions include the requester’s name, home or business address, personal or business email address, home or business telephone number, and a description of the requested records. Privacy Act transactions include:

a) FOI/Privacy Act Officer receives request
b) FOI/Privacy Act Officer or designee logs in request in to appropriate system
c) FOI/Privacy Act Officer assigns request
d) FOIA Specialist or assigned office conducts search for responsive records
e) FOIA Specialist or assigned office reviews records and redacts, as needed
f) Response and responsive records are released to requester
g) FOIA Specialist closes out request

Example 2:
Typical transaction

Privacy incident transactions can include any type of sensitive or non-sensitive personally identifiable information (PII). PII incidents are reported and tracked in accordance with Commerce policy following the published guidance. Information sharing conducted on case by case with a need to know basis within the agency and with other federal agencies as required by law, regulations and guidance. PII incident transactions include:

1. Employee, Contractor, etc. reports PII incident to bureau/operating unit (BOU) Computer Incident Response Team (CIRT).
2. BOU CIRT reports PII incident to DOC-CIRT.
3. For cyber related incidents DOC-CIRT notifies the Chief Privacy Officer (CPO), US Computer Emergency Readiness Team (US CERT), and notifies the BCPO within one (1) hour. For non-cyber related incidents, DOC-CIRT notifies the CPO and BCPO within one (1) hour.
4. Bureau Chief Privacy Officer (BCPO) evaluates incident and rates risk level.
5. BCPO closes low risk incidents and recommends closure to CPO for moderate and high incidents
6. BCPO notifies DOC-CIRT of updates and closure of the incident.
7. DOC-CIRT closes the PII incident with notification to US CERT, if applicable.

Information sharing

Information sharing is performed on a case by case basis with Commerce BOUs and other federal agencies.

Legal authority to collect

The authority to deliver, maintain and approve Department-wide programs for FOIA, Privacy, Open Government, FACA and Directives Management and serve as the focal point for collection and reporting of OPOG programs within the Department of Commerce is delegated to the Office of Privacy and Open Government in DOO 20-31 - SECTION 3, the Office of Privacy and Open Government.

Authority for maintenance of systems

The authority for OPOG programs include the following, with all revisions and amendments: 5 U.S.C. 552; E.O. 12024; E.O 12838; OMB Circular No. A-135; Section 204 of P.L.104-4; P.L. 92-463; 5 U.S.C. App; 5 U.S.C. § 552; Title 15 CFR, Part 4; E.O. 13392; 5 U.S.C. 552a; FISMA of 2002, 44 U.S.C. § 3541; OMB M-03-22; M-06-15; M-06-16; M-06-19; M-07-16; M-11-02, and M-15-01.

10) Office of Performance, Evaluation, and Risk Management (OPERM)

Typical transaction

Typical transactions that involve non-sensitive PII are ones in which:

a) U.S. Government Accountability Office (GAO) or DOC Office of Inspector General (OIG) contacts the Department to provide notification that an audit is being conducted which includes names and contact information for the audit team. OPERM stores this information in the system and responds to the GAO or OIG with the names of audit liaisons and Department staff who will work with the auditors.

b) Department or bureau staff contacts OPERM to request accounts in the Audit Management System (AMS). OPERM will send this information to the system administrator (a contractor) and request that accounts are set up, using a user name and email. The email may be used by the AMS to send automated email notifications. The user name is used to create a log-on ability.

c) Names and contact information for bureau and Department staff working with the Enterprise Risk Management and Performance programs are stored in the system and used to contact the individuals regarding program activities. Contact lists may be shared with other bureau and Department staff. For example, a NOAA employee may request the name(s) and contact information of NOAA staff with risk management or performance responsibilities.

Information sharing

OPERM staff may manually refer to records in the system for names and contact information stored in them and forward the information as needed within the course of performing our office missions. However, there is no automated sharing of OPERM information within the OITS-GSS.

Legal authority to collect

a) Enterprise Risk Management - The Federal Managers' Financial Integrity Act of 1982 (FMFIA); the Office of Management and Budget (OMB) Circulars A-123 and A-11, and other authorities cited in DAO 216-20, Enterprise Risk Management.

b) Performance Excellence Program and Performance Evaluation - Government Performance and Results Act (GPRA) Modernization Act of 2010, and OMB Circular A-11.

c) Office of Inspector General (OIG) / Government Accountability Office (GAO) Audit Liaison and Follow-up – the GAO Act of 1980, the Legislative Reorganization Act of 1970, OMB Circular A-50, and other authorities cited in DAO 213-1 GAO Liaison and Audit Follow-up.

d) Non-financial internal control implementation and management - Federal Managers' Financial Integrity Act of 1982 (FMFIA) and OMB Circular A-123.

11) Office of Security (OSY)

Typical transaction

The information is collected from federal employees, contractors, Departmental non-government personnel, and foreign nationals. The data is maintained in the system as a system of record and to verify existing data. The data is then used to determine if employment with the Department is viable. The information is maintained as historical information.

Information sharing

The data is disseminated to the Department of Justice (DOJ) and Office of Personnel Management (OPM) for the individual background checks.

Legal authority to collect PII and/or BII

DOO 20-6, 5 CFR 731, 5 CFR 732, Executive Orders (EO) 10450, 12968, 13488, 13467.

12) Office of Small and Disadvantaged Business Utilization (OSBDU)

OSBDU is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

13) Office of the CIO, Office of Cyber Security (OCS)

OCS is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

14) Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of Policy and Strategic Planning (OPSP)

OPSP is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

15) Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of IT Services (OITS)

Typical transaction

OITS obtains a user name which will be used to create a system account which includes the general support system and secure file transfer.

Information sharing

No information sharing is conducted by the system.

Legal authority to collect PII and/or BII

5 U.S.C. § 301, The Federal Records Act; The President's Memorandum on Transparency and Open Government, January 21, 2009; The OMB Director's Open Government Directive Memorandum, December 8, 2009.

16) Office of the Executive Secretariat

Office of the Executive Secretariat is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

17) Office of General Counsel (OGC)

Typical Transaction

OGC collects sensitive PII/BII from employees and contractors to support its daily mission. The information is used for operational purposes including: budgeting, human resources management, property management, travel management, and contract management. The information is collected via forms completed by employees and contractors and contract copies received for products and services acquired.

General Litigation receives claims via Government standard forms SF-91 and SF-95 electronically or by mail. Certain PII/BII is collected to review and process claims made against the government to determine whether payment is appropriate.

Information sharing

Administrative information is shared internally within the office. Litigation information is shared within the bureau, the US Government, and foreign entities.

Legal authority to collect PII and/or BII

Form 95 Authority to collect 5 U.S.C. 301, 28 U.S.C 501 et seq., 28 U.S.C. 2671., 28 C.F.R.

18) Office of Legislative and Intergovernmental Affairs (OLIA)

Typical transaction

The Office of Legislative and Intergovernmental Affairs collects Public/Government PII and sends it in to the White House or the Department of Commerce's White House Liaison's office through the secure file transfer system. The PII is collected so that the individuals requiring access to the White House may be processed.

Information sharing

Information is shared with the White House or Department of Commerce's White House Liaison Office.

Legal authority to collect PII and/or BII

DOO 25-4B Section 6.

19) Office of Public Affairs (OPA)

Typical transaction

The Office of Public Affairs (OPA) has the potential to store information, such as PII and BII to conduct the work of the office in setting up media interviews, disseminating public information as it pertains to the Department and its bureaus, and maintaining media lists and business contact lists. This PII and BII is usually stored as contacts, as a media list, database or as a stand-alone document. Only OPA staff members can access data entered by OPA staff and only OPA users can edit that data.

Information sharing

In a typical transaction, media contacts and outlets along with organization information is shared between OPA and the twelve Department of Commerce bureaus. This information may also be shared with other U.S. government agencies such as the White House, Department of Interior, etc. on an as needed basis.

Legal authority to collect PII and/or BII

DOO 15-3 Section 3
DAO 219-1 Sections 4, 5, 6, 7, 8, 9, 10, 11 and 14

20) Economic and Statistics Administration (ESA)

The ESA uses enterprise and network services to support their daily mission. The ESA does not collect, maintain or disseminate PII nor does the ESA collect, maintain or disseminate BII such as trade secrets, commercial information or financial information.

21) Economic Development Administration (EDA)

Typical transaction

The EDA downloads grant information from https://www.grants.gov. These downloads may contain sensitive and non-sensitive PII and BII data. These forms are grant applications for local and state governments, education organizations, public housing organizations, nonprofit organizations, for-profit organizations, small businesses, individuals and foreign applicants.

Additionally, the EDA's Office may collect, maintain and disseminate PII and BII in support of the Revolving Loan Fund Program. This program supplies small businesses and entrepreneurs with gap financing to start or finance businesses.

Information sharing

Grantor and applicant information is shared between Grants.gov and the EDA utilizing the Grants.gov System-to-System feature and the Revolving Loan Fund (RLF).

Legal authority to collect

The collection and maintenance of the BII data information for the Revolving Loan Fund (RLF) program is authorized by the Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Public Law(P.L.) 108-373).

22) Minority Business Development Agency (MBDA)

Typical transaction

The MBDA customer records management system captures the telephone numbers, names and email addresses of each business involved in transactions. This system also includes some personal information of the individuals such as name and phone number associated with the businesses, and source information about the businesses (financial information for contracts, loans, bonding; number of jobs created and retained; professional capacities and certifications such as SBA 8(a) and state minority certifications). MBDA's online tools also capture some BII, such as opportunities for contracts secured or pending in the private and public sectors; and communications between business centers and clients.

Information sharing

Information is shared by the forty-four (44) MBDA Business Development Centers with the MBDA Headquarters located in Washington, D.C.

Legal authority to collect

The authority for collecting the name, addresses, company size, transaction type and amounts, contract amounts, loan amounts, and jobs created of minority business enterprises that receive technical business assistance from the MBDA Business Centers (grantees) is provided in 2 C.F.R. Section 200.328(b)(1) of the Office of Management and Budget's (OMB) Rules for Grant Administration which provides in part: "[t]he non-Federal entity (grantee) must submit performance reports at the interval required by the Federal awarding agency."

The authority for MBDA's grant program is contained in Executive Order 11625, which authorizes the Secretary of Commerce to provide financial assistance to public and private organizations so that they may render technical and management assistance to minority business enterprises. The Secretary's authority was delegated to the National Director of MBDA in Section 3 of Department Organization Order (DOO) 25-4A, Minority Business Development Agency. The MBDA grant program is also authorized by 15 U.S.C. § 1512.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks.
__X__ This is an existing information system in which changes do not create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained or disseminated *(check all that apply).*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: OGC – SSN required as part of travel processing for repayment of vouchers. MBDA – SSN are sometimes received inadvertently through resumes for new hires, center directors, and clients of business centers. OCR – SSNs are no longer collected but some older records retained due to litigation holds contain them. OHRM – SSNs are used as a unique identifier, for a number of HR related systems.					

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

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. XJob Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

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

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

OCR – Narrative information regarding claims of discrimination.

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	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify):					

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

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed (*check all that apply*).

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	X
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

<u>Section 3:</u> 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	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation	X	For criminal law enforcement activities	
For civil enforcement activities	X	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): Grant program requirements			

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).

s.

In general, twenty-three (23) Business Operating Units (BOU) within DOC use OITS-GSS services for data storage and retrieval of program information supporting official daily responsibilities and the organization's mission. Information use is limited to: developing policies, managing programs and providing oversight for collaborative efforts with business customers. The official needs of the BOU determine the extent of the information sharing with other organizations.

The information is collected from federal employees, contractors, Departmental non-government personnel, and foreign nationals based on OITS-GSS customer missions. All information access is controlled based on user business roles which restrict the ability to view, copy, modify, and delete the information. The data is restricted for dissemination based on business office documented requirements in accordance with published guidelines.

The actual use of the GSS services is described in more detail in the “Typical Transaction” section under each BOU and below:

Economic and Statistics Administration (ESA)

ESA is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Economic Development Administration (EDA)

Grant applications/forms:

The forms used for the grants’ request requires the information. The information is used to determine eligibility.

Revolving Loan Fund (RLF) Program:

The type of business identifiable information (BII) contained in RLFMS is primarily financial data and could include business names, bank information, borrow loan account information, and additional grantee and borrower information. The information is collected to be in compliance with the semi-annual RLF reporting requirements.

Minority Business Development Administration (MBDA)

The Minority Business Development Agency uses potentially sensitive BII and race/ethnicity information collected from minority business enterprises to determine eligibility for participation as clients of the MBDA Business Center program. The information collected is from members of the public

MBDA maintains and collects PII when conducting HR actions such as hiring new employees. These are for administrative matters pertaining to contractors and federal employees.

Office of Business Liaison (OBL)

As part of our office’s responsibilities, we collect names and contact information for key individuals from the private sector and relevant industry associations. Part of the business processes include compiling the data in spreadsheets and using the information to extend invitations to relevant events hosted by DOC and/or set-up one-on-one meetings with members of the team. Collection and use of this data is critical to our office’s mission of representing private sector interests through strategic engagement.

Center for Faith Based and Neighborhood Partnerships (CFBNP)

CFBNP collects this information to bring people to meetings with White House staff that are focused on key Commerce and White House programming around economic development, job creation, business development, trade, and other areas of community improvement.

Office of Acquisition Management (OAM)

The information from System for Award Management (SAM) is used to fulfill policy requirements set forth by the FAR and to ensure that every action awarded to a vendor/contractor meets the needs and requirements of the Department of Commerce.

Office of Facilities and Environmental Quality (OFEQ)

Information collected is used for building user access tables to allow assignment of user privilege, and assignment of access passwords.

All information collected will be from federal employees. No contractors, foreign nationals, or visitor information will be collected.

Office of Budget (OB)

The information is collected from federal employees and transmitted to OMB. Federal security personnel for NEOB use the information to verify an attendees identify in order to grant access to the building. Meetings with the EOP are a necessary aspect of coordinating the preparation and presentation of the Department's annual budget request.

Office of Civil Rights (OCR)

EEO complaints are filed by employees of the Department and applicants seeking employment contact information for the complainant (attorney/representative/union representative) and representatives (OGC's attorney assigned to the case) for either the complainant or the Department. This provides both parties (individuals working with the complainant and the Department representatives) with the notices, reports, decisions, and supporting documents related to the complaint. A complainant is required to provide the demographic and employment information relevant to his or her claim of discrimination. This enables OCR to determine if the complaint meets procedural and/or jurisdictional requirements necessary to direct the scope of the investigation and adjudication of the complaint, which is directly related to OCR's core mission of enforcing nondiscrimination laws.

The BII maintained in OCR's systems contains contact information for law firms, unions and other agencies that represent each individual complainant. Other BII identifies the following: name of the firm contracted to investigate the case, name and contact information of the assigned subcontractor, and the costs associated with the investigation. This category of BII allows OCR to manage its investigative contracts to ensure costs allocated is controlled appropriately and the work is distributed in accordance with the contract statement of work. The contractors and subcontractors do not have access to OCR systems. They are, however vetted to ensure they qualify for the acquisition process related to the complaint filed. Once that process is completed and the contract has been awarded, the case is assigned to a case-worker.

PII and BII are disseminated only within the framework of administrative complaint processes, and/or related litigation in federal court. Information is provided to the OGC's Employment and Labor Law Division, EEOC, Merit Systems Protection Board and/or Assistant U.S. Attorneys on a case-by-case basis. PII may also be shared with the servicing Human Resources Office (SHRO) to the extent required to carry out personnel actions ordered as corrective action, or the agreed terms for settlement.

Statistical data from the system is annually provided to the EEOC, the Office of Personnel Management, the Department of Justice and selected members of Congress in compliance with The No Fear Act and the EEOC Form 462 report.

Office of Financial Management (OFM)

1. The purpose of the Passport and Visa database is to track and maintain official and diplomatic passports and visas for various bureau Federal employees, their spouses, dependents, or otherwise traveling with a DOC employee. The Department of State determines if an employee is eligible to receive a passport and the Travel Staff only records the reason for denial in the database.

2. The purpose of the JP Morgan Chase System is to manage the Department's Travel Card Program for Departmental Federal employees.

3. The purpose of the Sunflower Personal Property Management System is to maintain accountability of all personal property assets and fleet of vehicles across the Department for Federal employees and contractors.

4. 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.

Office of Human Resource Management (OHRM)

1. Automatic Classification System (ACS) contains key position data that supervisors use to create and simultaneously classify Demonstration Project position descriptions.

2. PPS information collected is intended to ensure accurate rating and ranking of CAPS employees' performance and based on the performance rating, calculate salary increase and bonus payout.

3. ERIS-TL information collected is intended to ensure that the most senior Departmental executives have access to accurate and up-to-date information as to the incumbency status of all key SES positions. It is also referenced in the course of key Departmental decision-making with regard to executive staffing.

4. SES Bonus Pool information collected is intended to ensure the accurate rating, pay adjustment and bonus information of SES employees compiled for the Departmental Executive Resources Board's (DERB) consideration.

5. HANS' intended use is for a more efficient and effective program administration for nominating an employee for gold and silver honor awards and a more efficient process of selecting and ranking the nominees.

6. WebTA is used to track DOC employees' hours; so, each employee can be paid or compensated accordingly.

Office of Privacy and Open Government (OPOG)

The PII/BII data will also be used to contact requesters, other federal agencies, and staff fulfilling requests for information, as well as by requesters following up on the status of their requests.

The PII/BII identified in Section 2.1 of this document is in reference to federal employees / contractors, members of the public and private entities.

In order to ensure protection of PII/BII OPOG tracks, maintains metrics, and reports PII incidents in accordance with OMB guidance. This reporting may contain various elements of PII for investigation and notification.

Office of Performance, Evaluation, and Risk Management (OPERM)

GAO & OIG Audit Liaison & Follow-up:

- Name and business contact information (telephone, email, business address) and job title of (a) Government Accountability Office (GAO) and Commerce Office of Inspector General (OIG) points of contact for audits and other engagements with GAO and OIG, and (b) Commerce and Commerce Bureau employees who participate in GAO and OIG engagements, or are stakeholders in the process, and (c) contacts at other federal agencies that we interact with in connection with Audit Liaison & Follow-up activities. The information is used for OPERM to contact the individuals. It may also be shared with Bureaus/Department Offices or with GAO and OIG for the purpose of advising them of points of contact or attendance at meetings.

Risk Management:

- Name and business contact information (telephone, email, business address) and job title of (a) Department and Bureau employees with a role in the Enterprise Risk Management

(ERM) process (such as Risk Management Officers and Enterprise Risk Management Council Members, (b) Commerce and Commerce Bureau employees who are stakeholders in the ERM process, and (c) contacts at other federal agencies who we deal with on interagency risk management efforts. This information may be shared with Bureaus/Department Offices for the purpose of advising them on points of contact or attendance at meetings.

Federal Financial Manager's Integrity Act (FMFIA) and Internal Controls:

- Email distribution list of individual names and email addresses to receive notices and instructions for completing an annual FMFIA report; bureau submission of business information summarizing its internal control and risk management activities.

Program Evaluation:

- Individual names and email addresses to provide instruction and guidance on program evaluations and reviews.

Performance Excellence:

- Individual names and email addresses to provide instruction and guidance on performance excellence.

Office of Security (OSY)

The information is collected from federal employees, contractors, Departmental non-government personnel, and foreign nationals. The data is maintained in the system as a system of record and to verify existing data. Fingerprint data is disseminated to DOJ for the individual background checks. SF 85 and SF 86 form data is disseminated to OPM. The data is then used to determine if employment with the Department is viable. The information is maintained as historical information.

Office of Small and Disadvantaged Business Utilization (OSBDU)

OSBDU is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of the Chief Information Officer (OCIO), Office of Cyber Security (OCS)

OCS is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of Policy and Strategic Planning (OPSP)

OPSP is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of IT Services (OITS)

The Office of Information Technology Services manages the HCHB digital network, telecommunications services, and network-enabled services, such as emergency broadcast, voice mail, and Internet Domain Name Service. The Office manages Department-wide telecommunications services, such as FTS2001 and WITS, and coordinates telecommunication and networking operations across the Department.

PII is collected from federal employees and contractors so that system accounts can be created on the GSS.

Office of the Executive Secretariat

Office of the Executive Secretariat is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of General Counsel (OGC)

OGC collects this information for disciplinary actions, position advancement, granting access for visitors of senior General Counsel staff, and to provide litigation services for the Secretary of Commerce and all Operating Units. This information is collected from federal employees, contractors, members of Public who visit commerce facilities.

Office of Legislative and Intergovernmental Affairs (OLIA)

The Office of Legislative and Intergovernmental Affairs collects Public/Government PII and sends it in to the White House or the Department of Commerce's White House Liaison's office through the secure file transfer system. The PII is collected so that OLIA staff members requiring access to the White House may be processed.

Office of Public Affairs (OPA)

The type PII/BII that is collected, maintained, or disseminated by the Office of Public Affairs includes the following:

- Business names
- CEO and business leader contact information
- Media organizations
- Reporter emails and phones
- Additional business/company information that may be important to disseminating Department information publically

- Additional media outlet or reporter information as it pertains to an interview request, event or engagement.

The information collected is pertinent to setting up media interviews, disseminating information as it pertains to the Department and its bureaus, and maintaining media and business contract list. Only information that is required for responding to a public information request, interview request or correspondence is collected and stored.

<u>Section 6:</u> 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	X	X
DOC bureaus	X	X	X
Federal agencies	X	X	x
State, local, tribal gov't agencies	X		X
Public	X		
Private sector	X		X
Foreign governments	X		
Foreign entities	X		
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.

	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:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII (*check all that apply*).

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system (*check all that apply*).

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	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: _https://www.commerce.gov/page/privacy-policy_.	
X	Yes, notice is provided by other means.	Specify how: ESA – Not collecting, maintaining, or disseminating PII/BIIEDA – Individuals are notified at the Grants.gov website by OMB which is not under the control of EDA. MBDA – Individuals are notified in the MBDA Business Center engagement form. OBL – Individuals are notified verbally during collection process by the OBL POC. CFBNP – Individuals are notified by the CFBNP POC that it is for WAVES purposes to provide to the White House and used to clear them to get into the building by the CFBNP POC. OAM – Individuals are notified during Sam.gov registration. OFEQ – Individuals are notified verbally during the collection process by the OFEQ POC. OB – Individuals are notified by OB POC that it is for WAVES and that their information will be provided to OMB to gain access to the NEOB by the OB POC. OCR – Individuals are notified on the Formal Discrimination Complaint Form. OFM – Individuals are notified in the JPMC Statement of Understanding and Agreement. OFM Data Analytics Program – Under initial collection for the following systems: WebTA, NFC, PaymentNet. OHRM – Individuals are notified via various HR forms at and before onboarding, both electronic and hard copy, and are provided notice via a header in WebTA.

		OPOG – Individuals are notified via web form, verbally, and through Privacy Notification by OPOG POC. OPERM – Individuals are notified via email and verbal communications by OPERM POC. OSY – Individuals are notified on the SF-86, SF-85, or SF85p. OSBDU –Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. Planning (OPSP) and Office of IT Services (OITS). OCIO, OCS - Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OPSP –Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OITS – Individuals are notified during interview process by OITS POC for gathering account information. OES – Not collecting, maintaining, or disseminating PII/BII. OGC –Notification is provided via the SF-95 form. OLIA – Individuals are notified during the collection process by the collector and/or DOC employee. OPA – Individuals are notified via email and verbal communications by OPA POC.
	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: ESA – Not collecting, maintaining, or disseminating PII/BII. EDA - Grant data: The individual can decline to provide the data. The individual has to provide information on the form to process their grant request. MBDA – Individuals can decline verbally or in writing to the MBDA or MBDA Business Center. OBL – Individuals can decline verbally to the OBL POC. CFBNP – Individuals can decline verbally to the CFBNP POC. OAM – Individuals can decline during Sam.gov registration. OFEQ – Individuals can decline via the application for parking. OB – Individuals have the ability to decline verbally to the OB Coordinating Analyst. OCR – Refusal to provide information relevant to the investigation and adjudication of the complaint may result in dismissal of the complaint. OFM – Individuals can decline by not signing the application and/or agreement. OFM Data Analytics Program – Under initial collection for the following systems: WebTA, NFC, PaymentNet. OHRM – Individuals can decline by not accepting the position of employment verbally or in writing to the OHRM POC.

		OPOG – Individuals can decline by not filling out web form or verbally with the OPOG POC. OPERM – Individuals can decline via email and verbal communications with the OPERM POC. OSY - Individuals can decline to provide the requested information online by not submitting the information. OSBDU – Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. OCIO, OCS - Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OPSP – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OITS – Individuals can decline by refusing to complete account request forms. OES – Not collecting, maintaining, or disseminating PII/BII. OGC – Individuals can decline to provide PII at the time of filling out SF-91 or SF-95. Denial of submitting certain PII could result in denial of claim. OLIA – Individuals may decline verbally or in writing to the OLIA POC. OPA – Individuals can decline verbally or in writing to the OPA POC.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: EDA – RLF data: No individuals will have the opportunity to decline providing information as there are currently no voluntary collections within RLFMS. Many parts of the data contained with RLFMS are mandatory and must be provided for proper use of reporting the RLF portfolios. Failure to provide the information may render it impossible for EDA to correspond with the requestor.

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: ESA – Not collecting, maintaining, or disseminating PII/BII. EDA - Grant data: The individual can decline to provide the data. The individual has to provide information on the form to process their grant request. MBDA – Individuals can decline verbally or in writing to the MBDA or MBDA Business Center. OBL – Individuals can decline verbally to the OBL POC. CFBNP – Individuals can decline verbally to the CFBNP POC. OAM – Individuals can decline during Sam.gov registration. OFEQ – Individuals can decline via the application for parking. OB – Individuals have the ability to decline verbally to the OB Coordinating Analyst. OCR – Refusal to provide information relevant to the

		investigation and adjudication of the complaint may result in dismissal of the complaint. OFM – Individuals can decline by not signing the application and/or agreement. OFM Data Analytics Program – Under initial collection for the following systems: WebTA, NFC, PaymentNet. OHRM – Individuals can decline by not accepting the position of employment verbally or in writing to the OHRM POC. OPOG – Individuals can decline by not filling out web form or verbally with the OPOG POC. OPERM – Individuals can decline via email and verbal communications with the OPERM POC. OSY - Individuals can decline to provide the requested information online by not submitting the information. OSBDU – Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. OCIO, OCS - Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OPSP – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OITS – Individuals can decline by refusing to complete account request forms. OES – Not collecting, maintaining, or disseminating PII/BII. OGC – Individuals can decline to provide PII at the time of filling out SF-91 or SF-95. Denial of submitting certain PII could result in denial of claim. OLIA – Individuals may decline verbally or in writing to the OLIA POC. OPA – Individuals can decline verbally or in writing to the OPA POC.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: MBDA - No separate distinction on use for particular purposes; e.g., transfer to ESA for studies or other uses.

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: ESA – Not collecting, maintaining, or disseminating PII/BII. EDA - Via the RLF program reporting process which is semi-annual. MBDA – Individuals can contact MBDA or their operating MBDA Business Center verbally or in writing OBL – Individuals can review/update through the Office of the Secretary Scheduling Office CFBNP – In writing to the CFBNP POC. OAM – Individuals can review/update at Sam.gov

		OFEQ – Employees notify the OFEQ POC when administrative PII requires updating. OB – Individuals provide their updated information directly to OB for transmission to OMB. OCR - Individuals can contact OCR compliance staff to review or add updates to their files. OFM - Over the phone and online to the PFM POC. OFM Data Analytics Program – Data has been previously collected from users through other systems and/or applications. Data received for this program is for analysis only and not changes can be made to it once received by OFM. OHRM – Individuals update via their employee official personnel file (e-OPF) via their online account. OPOG - Through the Privacy Act individuals have the opportunity to review/update PII/BII pertinent to them. They can submit updated web forms. OPERM - Individuals provide updated contact information by email, phone, or hard copy to the OPERM POC. For information maintained in contact lists, updates are periodically requested by the OPERM POC. OSY – Individuals may contact Human Resources personnel to review or update their personal information. OSBDU – Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. OCIO - Employees notify the OCIO POC when administrative PII requires updating. OCS – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OPSP – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OITS – they resign the acceptable use policy on the annual basis where they are required to verify their information OES – is not collecting, maintaining, or disseminating PII/BII OGC – Individuals can review and update their PII online via electric online personnel file (EOPF) OLIA – OLIA is only forwarding the information provided by the applicant. OPA – Verbally and in writing to the OPA POC
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

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: OFM Data Analytics Program – Contractor access is limited to contractor staff who have signed non-disclosure agreements and are escorted by OFM staff, after signing-in and clearing security to enter the building. Access is monitored by physical observation by OFM staff. Laptop is located in a secure section of the building with auto-locking doors before and after core working hours. In addition, the area has security cameras which are monitored by building security.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 7/19/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The OITS-GSS systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in-transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS) • 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 (NIST) standards, including special publications 800-53, 800-63, 800-37, etc. Any system within the organization that contains, transmits or processes BII/PII 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. All databases containing sensitive PII must encrypt data at rest and ensure use of HTTP(S) for public-facing websites. All databases under OCIO control with PIA (e.g., Microsoft Office 365 data) are encrypted at rest. The organization also employs data loss prevention (DLP) solutions as well. The DLP is an e-mail scan of unencrypted e-mail traffic, to included attachments.

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 **COMMERCE/DEPT 1 – 23,** COMMERCE /DEPT-1—Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE /DEPT-2—Accounts Receivable COMMERCE /DEPT-3— Conflict of Interest Records, Appointed Officials COMMERCE /DEPT-4— Congressional Files COMMERCE /DEPT-5— Freedom of Information and Privacy Request Records COMMERCE /DEPT-6— Visitor Logs and Permits for Facilities Under Department Control COMMERCE /DEPT-7— Employee Accident Reports COMMERCE /DEPT-8— Employee Applications for Motor Vehicle Operator's Card COMMERCE /DEPT-9— Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE /DEPT-10— Executive Correspondence Files COMMERCE /DEPT-11— Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees COMMERCE /DEPT-12—OIG Investigative Records COMMERCE /DEPT-13— Investigative and Security Records COMMERCE /DEPT-14— Litigation, Claims, and Administrative Proceeding Records COMMERCE /DEPT-15— Private Legislation Claimants-Central Legislative Files COMMERCE /DEPT-16— Property Accountability Files COMMERCE /DEPT-17— Records of Cash Receipts COMMERCE /DEPT-18—Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE /DEPT-19— Department Mailing Lists

	COMMERCE /DEPT-20— Biographical Files and Social Networks COMMERCE /DEPT-22— Small Purchase Records COMMERCE /DEPT-23—Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs **EEOC GOV-1** EEOC /GOVT-1—Equal Employment Opportunity in the Federal Government Complaint and Appeal 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: **National Archives and Records Administration (NARA) General Record Schedules –** General Record Schedule 1, General Record Schedule 3, General Record Schedule 9, General Record Schedule 14, General Record Schedule 16, General Record Schedule 18, General Record Schedule 23
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII (*check all that apply*).

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Pubication 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.
	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 levels (*check all that apply*).

X	Identifiability	Provide explanation: Certain PII is uniquely and directly. Identifiable.
X	Quantity of PII	Provide explanation: Large PII datasets are present on the system.
X	Data Field Sensitivity	Provide explanation: Certain combinations of system PII data fields are sensitive.
X	Context of Use	Provide explanation: OFM Data Analytics Program – Statistical analysis will be performed on the data collected from each system.
	Obligation to Protect Confidentiality	Provide explanation: OFM Data Analytics Program – Any 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.
X	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

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

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.