Template Version Number: 01-2021

U.S. Department of Commerce
Office of Financial Management Systems (OFMS)

Privacy Impact Assessment
for the
Business Applications Solution (BAS) OS-077

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

Tahira Murphy — Digitally signed by Tahira Murphy Date: 2022.08.11 16:10:01 -04'00' — for Jennifer Goode — 8/11/2022

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

U.S. Department of Commerce Privacy Impact Assessment
OFMS/Business Applications Solution (BAS) OS-077

Unique Project Identifier: BAS OS-077

Introduction: System Description

Provide a brief description of the information system.

The Business Applications Solution (hereby referred to as BAS or BAS OS-077) project is a U.S. Department of Commerce (DOC) modernization initiative to deploy an integrated suite of financial and business management applications to support its mission. BAS is responsible for implementing and integrating a suite of commercial off-the-shelf (COTS) business systems, enterprise data warehouse (EDW) and business intelligence (BI) reporting solution, and system interfaces in a hosted environment. Business systems include the department's Core Financials Management Systems, Acquisition, and Property Management systems.

The Secretary of Commerce identified BAS as one of the top Departmental priorities. BAS consists of multiple Cloud Service Provider (CSP) services to deliver a holistic solution to DOC. BAS includes the following FedRAMP approved CSP solutions: Enterprise Data Warehouse (EDW), ServiceNow (SNOW), Xtended Detection and Response (XDR) Managed Security Services, Accenture Federal Cloud Enterprise Resource Planning (AFCE), Unison PRISM, Sunflower Personal Property Management System, Tenable.io, Dynatrace, and DocuSign.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
BAS OS-077 is a major application supporting all bureaus at the Department of Commerce.

(b) System location
(c) BAS consists of multiple FedRAMP Authorized cloud service provider (CSP) offerings. Each of these offerings are located in cloud data centers in the United States. Additionally, BAS uses availability zones spread across multiple redundant data centers. If one zone fails, or has some other interruption, the next availability zone seamlessly picks up. Therefore, data could be processed in any one of the zones at any given snapshot in time.

(d) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The BAS project is a U.S. Department of Commerce modernization initiative to deploy an integrated suite of financial and business management applications to support its mission.

BAS consists of multiple FedRAMP Authorized cloud service provider (CSP) offerings. BAS is comprised of the following CSPs:

- Enterprise Data Warehouse (EDW)
- Accenture Insights Platform (AIP) for Government Platform as a Service (PaaS)
- ServiceNow Government Community Cloud (SaaS)
- Xtended Detection and Response (XDR) for Government (SaaS)
- Accenture Federal Cloud Enterprise Resource Planning (AFCE)
- Unison PRISM (PRISM)
- Sunflower Personal Property Management System (Sunflower)
- Tenable.io
- Dynatrace
- DocuSign

BAS also connects with a number of Department and external systems. These connections are governed within applicable ISAs. Systems that BAS currently has an ISA:

- **Department of Commerce Systems**
  - NOAA 1101
  - NOAA 0700 NOAA ICAM
  - NIST HR CPR 183-01
  - NIST PO CBS 162-02
  - NIST ANTS 181-01
  - Census CBS 2781
  - Census CHAS CBS 2781
  - ITA Network Discovery 2645
  - OFMS Enterprise Applications System (EAS) OS-059
  - HCHBNet OS-003
- **External Systems**
  - Carson Wagonlit CWTSato Travel
  - U.S. General Services Administration GSAFleet.gov
  - U.S. General Services Administration GSAXcess
  - USDA NFC Enterprise Infrastructure and Platforms (NFC-EIP) 1040
  - Citibank SmartPay3
  - WEX Inc. SmartPlay3
  - Department of Treasury, Treasury Web Application Infrastructure (TWAI)
  - E2 Solutions

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

The BAS project is a U.S. Department of Commerce modernization initiative to deploy an integrated suite of financial and business management applications to support its mission. BAS is responsible for implementing and integrating a suite of commercial off-the-shelf (COTS) business systems, enterprise data warehouse (EDW) and business intelligence (BI) reporting solution, and system interfaces in a hosted environment. Business systems include the department's Core Financials Management Systems, Acquisition, and Property Management systems.

The Secretary of Commerce identified BAS as one of the top Departmental priorities. The objectives include implementing and integrating a suite of commercial off-the-shelf (COTS) business systems, enterprise data warehouse (EDW) and business intelligence (BI) reporting solution, and system interfaces in a hosted environment. The BAS Program will continue the ongoing emphasis on achieving organizational excellence and outstanding customer service for the Department. BAS consists of multiple Cloud Service Provider (CSP) services to deliver a holistic solution to DOC. BAS includes the following FedRAMP approved CSP solutions: Enterprise Data Warehouse (EDW), Accenture Insights Platform (AIP), ServiceNow (SNOW), Xtended Detection and Response (XDR) Managed Security Services, Accenture Federal Cloud Enterprise Resource Planning (AFCE), Unison PRISM, Sunflower Personal Property Management System, Tenable.io, Dynatrace, and DocuSign. The following sections describes the role of each solution in the BAS Solution set.

(f) How information in the system is retrieved by the user

Users are not authorized to access their data directly in BAS. If a user would like to review or edit the data that is transferred to BAS, the user must update it within the respective application.

(g) How information is transmitted to and from the system

Information is transmitted across approved encryption protocols such as HTTPS, SSH, and SFTP. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 180-1, and Secure Hash Standard issued by NIST when necessary.

(h) *Any information sharing*

Currently, no information sharing is conducted by BAS.

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

The following are programmatic authorities:
Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966)
Includes the following, with all 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; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 202-430 (performance management system), DAO 205-16 management of electronic records. The authority to deliver, maintain, and approve Department-wide and bureau-specific automated human resources systems and serve as the focal point for the collection and reporting of human resources information within the Department of Commerce (DOC) is delegated to the Office of Human Resources Management (OHRM). This authority is identified by Departmental Organization Order (DOO) -- 20-8 - SECTION 4.

(j) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
BAS is categorized as 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.
__X_ _This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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

____ 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.

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	f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card	X	m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify): • User IDs specific to administrative application sending data to BAS (e.g., E2 User ID, moveLINQ User ID, WebTA User ID) • Traveler Number, Traveler Redress Number					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Social security number is the only employee identifier that is consistent across E2 Solutions, moveLINQ, and WebTA, and NFC (i.e., same value represents an entity across systems). Consistent identifiers are					

required to integrate data/transactions associated to an employee across systems. Social Security Number is only used in backend data association processes. Social Security Number is not displayed in frontend reports. SSN is stored in the backend databases supporting EDW.

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

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	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): • Department • Office • Grade • Accounting Code Structure • Leave Balance / Travel Expenses / Relocation Expenses					

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	X	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): PII data from the individual is captured directly in the administrative systems, which send data into BAS. No PII data is entered directly from the individual into BAS.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): The following Government Source administrative systems send data, including PII/BII data, to BAS via SFTP: • moveLINQ (under EAS OS-059) • WebTA (under EAS OS-059) • NFC • NOAA CBS • NOAA1101 HR • NIST HR • NIST PO • NIST ANTS • Census CBS • Census CHAS • Census ITA • Sunflower Mobile (under EAS OS-059) • GSA SAM					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	X
Third Party Website or Application					
Other (specify): The following Non-Government Source administrative systems send data, including PII/BII data, to BAS via in via SFTP: • E2 Solutions • CWTSato Travel • WEX • CitiBank					

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

Data is ingested into BAS directly from the source systems. If the data that is ingested is incorrect, data must be updated at the source system.

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 is 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	X
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):Analytics and Reporting			

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 BAS EDW application ingests and integrates data from DOC administrative applications for financial, asset, acquisition, grants, HR, and travel management applications, to enable BI reporting and management insights on DOC business operations and metrics.

PII/BII information pertains to DOC employees that enter transactions in the following administrative systems:

- E2 Solutions – travel details, authorizations, vouchers, and payments
- moveLINQ – relocation details, advances, expenses, and payments
- WebTA – time charging details, and leave balances
- NFC – personnel and payroll data

Data is captured in administrative systems and sent to BAS EDW for BI (spell BI) reporting.

The BAS EDW application is used by DOC staff in administrative offices (Financial, Budget, Asset/Property, Acquisitions, Grants, HR, and Travel Management Offices) at the Department, Bureau, and Operating Unit levels. Access to PII data will be restricted to authorized users which requires access to perform required responsibilities (e.g. HR or Budget staff).

PII data elements will only be:

- ingested and/or displayed on a report if required to support business operations (e.g. Workforce Reporting & Analysis)

- have access restricted to authorized users in a role which requires access to such data to perform a mandatory administrative function (e.g. HR or Budget support staff)

SUNFLOWER

The PII identified in Section 2.1 is in reference to federal employees and contractors/associates in connection with their working relationship with BEA, BIS, Census, EDA, ESA, ITA, MBDA, NIST, NOAA, NTIA, and NTIS. The data will be used for purposes of providing access to delivering better services, and for carrying out of property and asset management activities. User information will be transferred securely from the bureaus to PPMS for more accurate user and account administration

AFCE

The following files / data from NOAA will be requested to support different BAS testing efforts including Conversion and System / Integration testing phases:

- SAM File: SAM V3 Production file (GSA data file)
- NOAA Corp: 1) Labor 2) Employees
- NFC Employee File
- NFC Labor File
- FOMF (Treasury Fiscal Services / PAM data file)
- DNP
- Pay.Gov, CIR (Treasury Fiscal Services data files)
- SISP
- ASAP, (Treasury Fiscal Services data files)
- GEMS (This eRA data files)
- SP3
- ETS2
- moveLINQ
- WebTA
- PAM (Treasury Fiscal Services data files)
- Legacy Data: PRISM, CFS / NDW, Sunflower transactional data including customers, vendors, employees, accounting reference data, general ledger / trial balances, projects, tasks, agreements, receipts, bills, receiving tickets, obligations, invoices, payments, etc.

Systems integrations include:

- Outbound Data Service: Accounting Reference Data – Bureau systems will retrieve accounting reference data from the BAS Financial Management Application (Oracle E-Business Suite (EBS)) in order to populate Standard Import Interfaces
- Standard Import Interfaces – Bureau systems will send financial transactions to BAS EBS for processing and update of financial accounts
- Outbound Data Service: Financial Transactions – Bureau systems will retrieve financial transactional data from the BAS Enterprise Data

Warehouse (EDW) to support bureau system functionality

PRISM
Information is collected in the System for Award Management (SAM) and then passed to PRISM for financial and business decisions. Any individual or company wishing to do business with the Federal Government must submit information into SAM to be considered for a contract or award. Any notification regarding use, collection, review, or updates to PII/BII is delivered by the SAM application. PRISM is updated on a daily basis with the applicable data from SAM. No individual or company has access to their information in PRISM. Information is required as part of the federal acquisition process for services, goods, and materials provided by the vendor community to the Federal Government. Having the correct Tax Identification Number (TIN) in System for Award Management (SAM) improves data collection by allowing a single point of data entry for any person or firm who wants to conduct business with the Federal Government.

The SAM web application is used by various departments and bureaus across the Federal Government. Since October 1, 2003, it is federally mandated that any person or firm wishing to conduct business with the Federal Government under a FAR-based contract must be registered in SAM before being awarded a contract [Federal Acquisition Regulation (FAR) policy FAR 4.1102 (October 1, 2003), and Federal Acquisition Circular (FAC) 2001-16]. In addition, this information is used in the DoC's Core Financial System to make timely payments to these vendors for their services and materials. DOC uses the information for the acquisition of and payment for goods and services by NOAA, Census, OS and NIST to support their respective missions. DOC shares this data as required by the Federal Acquisition Regulation (FAR).

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.)

Data collected by BAS is retained for at least three years per applicable GRS schedules. After this time, the data will be processed through existing DOC or Federal mandated data shredding and disposal processes or archived and placed inappropriate secure archival storage. Related training is held as part of annual DOC security training. Please see this web page: https://connection.commerce.gov/reference-and-other-resources/annual- cybersecurity-awareness-training. There is the potential for insider threat. Employees acting with higher privileges, are "classified" as "positions of trust." They receive training as a part of the annual security training on how to operate with privileged access and viewing PII. Each role has certain permissions allowing for the job

associated with it to be completed successfully. When a user is assigned to one of these roles, permissions are granted on a need-to-know basis. They are in a position of trust and are expected to perform quality control based upon their specific role. All information containing PII or elements of information that can be used to identify individuals must be transmitted in a secure method (Kiteworks, SFTP, etc.) as required. User access to the various permissions in BAS is audited regularly.

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			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

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?

	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.
X	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 toprocess PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII

	leakage: • E2 Solutions MIS extract • moveLINQ. • WebTA • National Finance Center (NFC) Payroll/Personnel System (PPS) extract • NOAA CBS • NOAA1101 HR • NIST HR • NIST PO • NIST ANTS • Census CBS • Census CHAS • Census ITA • Sunflower Mobile • E2 Solutions • CWTato Travel • WEX SmartPay3 • CitiBank SmartPay3 • GSA SAM Information is transmitted across approved encryption protocols such as HTTPS, SSH, and SFTP. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 180-1, and Secure Hash Standard issued by NIST when necessary.
	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, ordisseminated by the system. *(Check all that apply.)*

	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: Notice of collection is the responsibility of the source systems. BAS ingests the data from the individual source systems. Users do not have access to their data within BAS,
	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: If a user declines to have their data in one of the source systems, it will not be fed into BAS EDW.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses oftheir 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: If a user declines to have their data in one of the source systems, it will not be fed into BAS.

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users have the ability to review their data in the source systems. Users do not have the ability to access their data within BAS.
	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 thatapply.)*

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: Each of the individual applications within BAS have the ability to track access to all data and generate logs and reports.

X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. ATO Date: August 18th, 2021
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).

Data is encrypted in transit to from the source systems using FIPS 140-2 approved algorithms through SFTP. When the data is stored within the BAS system, it is encrypted at rest using FIPS 140-2 approved algorithms.

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 coveredby 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 whichinformation 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)*: • DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons • DEPT-2, Accounts Receivable

	• DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons • DEPT-16, Property Accountability Files • DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies • DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations
	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 andmonitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 2.4, item 030, and GRS 2.2, item 010, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify):			

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 theFederal 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: Specific individuals are able to be identified
X	Quantity of PII	Provide explanation: The PII contained in BAS is collected from all Commerce employees
X	Data Field Sensitivity	Provide explanation: Data collected contains various PII including SSN
X	Context of Use	Provide explanation: Data is used by DOC staff in administrative offices (Financial, Budget, Asset/Property, Acquisitions, Grants, HR, and Travel Management Offices) at the Department, Bureau, and Operating Unit levels
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974 (5 USC 552a) and OMB Memorandum provide the obligation to the US Government to protect this information
X	Access to and Location of PII	Provide explanation: Data is stored within a secure enterprise data warehouse, encrypted at rest in the BAS platform on AWS GovCloud and OCI GovCloud
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the informationcollected 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 sourcesother than the individual, explain why.)

After a review of the threats associated with the application, it was determined that since this application is primarily used for administrative support, a potential risk of insider threat was noted. To protect against this, each user is provided with annual cyber security training that outlines how to maintain and access systems with PII. Also, role-based protections are in place to ensure that users can access data that is only allocated to their bureau/role/level. Audit logs are captured in the system and provided to XDR for real time alerting and analysis.

12.2 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.

12.3 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.