Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Business Applications Solution (BAS) OS-077

U.S. Department of Commerce Privacy Threshold Analysis

OFMS/BAS OS-077

Unique Project Identifier: BAS OS-077

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The 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 is a major application supporting multiple bureaus at the Department of Commerce.

b) *System location*
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.

c) *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 CSP including:

- 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 Interconnection Security Agreements (ISA). Systems that BAS currently has an ISA include:

- **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)

d) *d) The purpose that the system is designed to serve*

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 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 COTS business systems, enterprise data warehouse (EDW) and 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.

.

e) The way the system operates to achieve the purpose

Enterprise Data Warehouse (EDW)

DOC requires the development and implementation of an Enterprise Data Warehouse (EDW) that allows DOC to take advantage of the Business Intelligence (BI) technology currently available in the marketplace. This solution will replace multiple disparate data stores and reporting solutions currently in place at various bureaus within DOC. The EDW will also contain data from the entire department.

Within the EDW solution, following DOC reporting challenges will be addressed:

- Extensibility
- Sustainability
- Consistency and redundancy
- Accessibility
- Performance and scalability
- Flexibility

The EDW technology design solution will meet the data warehouse objectives provided by DOC. The justification for tools and technology recommendations will be documented with the benefits of the usage of the technology within EDW. The technology platform will be comprised of:

- Data Lake to store all types of incoming, transformed, and curated data.
- Data Integration platform where incoming data will be cleansed, quality checked before transformation, distributed, and curated.
- Business Intelligence, data visualization, and analytics platforms with capabilities of reporting, dash boards, analytics that will meet DOC's analytics objectives.
- Any ancillary and/or supporting tools and technologies will be included in EDW and Reporting solution to provide the user interfaces and/or data distribution mechanisms to meet DOC's analytics objectives.
- The solution will meet all application and data Federal security standards.
- All tools and technologies in EDW solution will be in AWS GovCloud, FedRAMP certified, managed and maintained by Accenture Insight Platform (AIP).

The BAS EDW & BI Architecture Design required to support the identified capability needs is described below following architecture components:

- BAS EDW is designed with Cloud Infrastructure architecture
- Data Storage Platform
- Data Management Tools
- BI Reporting & Analytics Tools

- ETL tool Informatica for extraction / transformation / loading of disparate data sets
- Amazon managed Relational Data Store (RDS) Oracle Database
- Amazon Redshift Data Warehouse a fully managed, petabyte-scale data warehouse service in the cloud
- Platform Interface Mechanisms

Accenture Insights Platform (AIP)
AIP is designed to automatically create, host, monitor and manage client's analytical and big data environments. AIP enables Data Scientists and Data Artisans to set up the Analytics environment with powerful toolset and comprehensive data integration platform. The platform helps the Data Scientists to define the predictive analytic models, apply them on the defined data sets, and process the outcome without bothering about the underlying infrastructure setup and management.

ServiceNow (SNOW)
BAS utilizes a cloud instance of ServiceNow to serve as the Information Technology Service Management (ITSM) ticketing solution and the front-end portal for all BAS users. All BAS users will access the portal through ServiceNow and authenticate to the future-state Identity and Access Management (IDM) solution to receive access to the other cloud solutions.

Xtended Detection and Response (XDR)
BAS utilizes XDR to provide managed security services in terms of audit log review and incident detection for all the cloud solutions. Logs will be sent to the XDR platform from each of the CSPs for review of anomalies and incidents. XDR will provide metrics and alerts to the BAS security and BAS leadership through automation and dashboard reporting.

Accenture Federal Cloud Enterprise Resource Planning (AFCE)
AFCE is a secure cloud offering delivering virtualized back-office ERP solutions to U.S. Federal customers. The technical architecture for AFCE includes the installed software, infrastructure, and integration required to support both the implementation of the project applications as well as the long-term production support. The overall AFCE solution consists of key integration components to support the processing and tracking of financial transactions.

Unison PRISM (PRISM)
PRISM is a powerful, web-based application that provides federal and defense acquisition communities with the tools needed to effectively support the complete acquisition management lifecycle, from initial planning and requisitioning through source selection, award, post award management, and closeout. PRISM brings together key stakeholders – the program office staff, contracting professionals, and financial managers – and links them as a community for greater efficiency, productivity, and operational transparency.

Sunflower Personal Property Management System (Sunflower)
Sunflower is a COTS application that is used by the Bureaus to track and manage its Fleet, Personal and Real Property from acquisition through disposal and provide DOC with an automated data management inventory system for its real property holdings. It was designed to promote improved real property accountability and to assist in the more efficient and economical use of the DOC's real property assets.

Tenable.io
The Tenable.io system is a cloud-delivered cybersecurity solution that features dashboard visualizations, risk prioritization, and seamless integrations with third-party solutions. Tenable.io leverages Nessus sensors, active scanners, agents, and passive network monitoring for maximum scanning coverage across an organization's infrastructure. Common tasks, such as configuring scans, running an assessment, and analyzing results are user-friendly with the pre-defined scan templates and configuration audit checks that follow best practices frameworks, such as Center for Internet Security Benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).

Dynatrace
Dynatrace offers a software intelligence platform, purpose-built for the enterprise cloud. As enterprises embrace the cloud as the means for digital transformation, Dynatrace's all-in-one intelligence platform addresses the growing complexity that technology and digital business teams face. Dynatrace's platform does so by utilizing artificial intelligence and advanced automation to provide answers, not just data, about the performance of applications, the underlying hybrid cloud infrastructure, and the experience of its customers' users.

DocuSign
DocuSign Federal provides electronic signature technology and Digital Transaction Management services to facilitate electronic exchanges of contracts and signed documents. DocuSign's features include authentication services, user identity management and workflow automation. Signatures processed by DocuSign are comparable to traditional signatures based on the product's compliance with the ESIGN Act as well as the European Union's Directive 1999/93/EC on electronic signatures. DocuSign Federal is a SaaS application oriented towards federal government entities.

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

Enterprise Data Warehouse
Data ingest from the following DOC administrative applications:

E2 Solutions MIS extract: Data related to employee travel – trip information and expenses. PII data elements include:

- IN: Social Security Number, E2 Profile ID, Traveler Number, Travel Redress Number, Passport Number, Bank Account Number, Travel Credit Card Number, Trip ID
- GPD: Name, Date of Birth, Gender, Home Email, Home Phone
- WRD: Department, Agency, Organization, Grade, Office Email, Office Phone,
- Emergency Contact, Accounting Code Structure, Travel Expenses

moveLINQ Standard Data Output (SDO): Data related to employee relocation – relocation information and expenses. PII/BII data elements include:

- IN: Employee ID, TaxID, Relocation ID
- GPD: Name, Old/New Address, Email, Phone
- WRD: Department, Bureau, Office, Grade, Old/New Duty Address

- Family, Accounting Code Structure, Relocation Expenses

WebTA canned report extracts: Data related to employee time charging and leave balances. PII data elements include:

- IN: Social Security Number, WebTA User ID
- GPD: Name
- WRD: Organization, Email
- Accounting Code Structure, Leave Balance

National Finance Center (NFC) Payroll/Personnel System (PPS) extract: personnel and payroll ata

- IN: Social Security Number
- GPD: Name, Gender, Citizenship, Date of Birth, Education
- WRD: Department, Agency, Organization, Position/Title, Grade, Salary, Work History, Performance Rating, Phone

AFCE/EBS

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

PRISM

- The interconnection from BAS to GSA will cover two different integrations. SAM Contract Opportunities is a one-way communication where PRISM sends solicitation and award data to SAM. SAM Entity is a bi-directional integration where PRISM sends a request to add or refresh a vendor, and SAM responds with the appropriate data that is then updated in PRISM.
- The interconnection is one way communication from BAS to GSA. DOC will use BAS PRISM to create solicitations and awards which will be posted to SAM.gov. Federal Procurement Data System (FPDS) will also be used to integrate with PRISM system to populate a contract.

SUNFLOWER

- The data transferred may contain business or personally identifiable information (PII) and may include information such as bank routing and account numbers, Tax Identification Number, Social Security numbers, name, home addresses, birth dates, etc.

g) *Identify individuals who have access to information on the system*
BAS is restricted to only authorized CSC Contractors developing BAS as the system is currently in development. In the future access to PII data will be restricted to DOC users in a role which requires access to such data to perform required responsibilities (e.g., HR or Budget staff).

h) *How information in the system is retrieved by the user*
Users are unable 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.

i) *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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes	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. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

__X__ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

__X__ DOC employees
__X__ Contractors working on behalf of DOC
____ Other Federal Government personnel
_X___ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

__X__ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. The Social Security Number (SSN) is the only employee identifier that is consistent across E2 Solutions, moveLINQ, and WebTA (i.e. same value represents an entity across systems). Consistent identifiers are required to integrate data/transactions associated to an employee across systems. SSN is only used in backend data association processes. It is not displayed in frontend reports. SSN is collected from GSA SAM as individuals may use SSN in place of Tax ID for single proprietor businesses.
Provide the legal authority which permits the collection of SSNs, including truncated form. • The following legal authorities permit the collection of SSN: 5 U.S.C. 301; 44 U.S.C. 3101; Executive Office (E.O.) 12107, E.O. 131614, 41U.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.

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X___ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the BAS OS-077 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the BAS OS-077 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information Technology Security Officer Name: Eduardo Macalanda Office: DOC OFMS Phone: 301-355-5987 Email: emacalanda@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: EDUARDO MACALANDA Digitally signed by EDUARDO MACALANDA Date: 2022.07.25 16:32:01 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Densmore Bartley Office: OS OCIO Phone: 202-482-3186 Email: dbartley@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DENSMORE BARTLY Digitally signed by DENSMORE BARTLY Date: 2022.07.29 14:56:23 -04'00' Date signed: _____
System Owner Name: Teresa Coppolino Office: DOC OFMS Phone: 301-355-5501 Email: tcoppolino@doc.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: TERESA COPPOLINO Digitally signed by TERESA COPPOLINO Date: 2022.07.26 08:42:35 -04'00' Date signed: _____	**Authorizing Official** Name: Dr. Lawrence W. Anderson Office: OS OCIO Phone: 202-482-2626 Email: landerson@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2022.07.29 16:15:26 -04'00' Date signed: _____
Authorizing Official Name: Stephen M. Kunze Office: Office of Financial Management Phone: 202-482-3709 Email: skunze@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: STEPHEN KUNZE Digitally signed by STEPHEN KUNZE Date: 2022.07.26 10:56:31 -04'00' Date signed: _____	**Privacy Act Officer** Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Tahira Murphy Digitally signed by Tahira Murphy Date: 2022.08.05 08:44:59 -04'00' Date signed: _____

Bureau Chief Privacy Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Tahira Murphy Digitally signed by Tahira Murphy Date: 2022.08.05 08:47:54 -04'00' Date signed: _____	