Privacy Threshold Analysis
for the
Business Application
Solutions (BAS) OS-077
U.S. Department of Commerce Privacy Threshold Analysis

Business Application Solutions (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 and its purpose: Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:

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).

a) Whether it is a general support system, major application, or other type of system

Business Application Solutions or BAS OS-077 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. For the current state of BAS, it is comprised of the following CSPs:
- Accenture Insights Platform (AIP) for Government Platform as a Service (PaaS)
- ServiceNow Government Community Cloud (SaaS)
- Accenture Federal Services – Accenture Extened Detection and Response (XDR) for Government (SaaS)

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

BAS Enterprise Data Warehouse (EDW) receives data ingests from the National Finance Center (NFC), WebTA, moveLINO (Relocation), and E2 Solutions. These connections are governed within applicable Interconnection Security Agreements (ISAs).

d) The purpose that the system is designed to serve

The Business Applications Solution (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 BAS Program will continue the ongoing emphasis on achieving organizational excellence and outstanding customer service for the Department. BAS will consist of multiple Cloud Service Provider (CSP) services to deliver a holistic solution to DOC. For the current state of BAS, BAS will include three CSP solutions, Enterprise Data Warehouse (EDW), ServiceNow (SNOW), and Xtended Detection and Response (XDR) Managed Security Services.

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, dashboards, 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
ServiceNow (SNOW)
BAS will be utilizing 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.

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

All BAS users currently access the system using OpenVPN using multifactor authentication (MFA)

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Currently EDW will be the only BAS solution ingesting PII
For the initial ATO, BAS EDW functionality includes:
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

g) Identify individuals who have access to information on the system
Currently, BAS is restricted to only development users as the system is currently in development. In the future, access to PII data will be restricted to 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

Individuals 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.e., If webTA data stored in BAS needs to be updated, the edit of the data must occur in webTA, not in BAS.) All BAS development users currently access the system using OpenVPN using multifactor authentication (MFA). Once BAS Bureau users are added to the system, access to the data will be limited by role, bureau, and/or group (HR, budget, etc.)

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?

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

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

   ___ 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 (version 01-2015 or 01-2017). *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 (version 01-2019 or later). *Skip 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 (version 01-2019 or later). *Skip questions and complete certification.*

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

   **X** 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.

   ___ 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.)

<table>
<thead>
<tr>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
</tr>
<tr>
<td>Video surveillance</td>
</tr>
<tr>
<td>Other (specify)</td>
</tr>
<tr>
<td>Building entry readers</td>
</tr>
<tr>
<td>Electronic purchase transactions</td>
</tr>
</tbody>
</table>

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.)."

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

X 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.

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

   [Provide an explanation for the business need requiring the collection of SSNs, including
   truncated form. Social security number 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. Social Security Number is only used in backend data association processes. Social Security Number is not displayed in frontend reports.]


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 WebTA-ArchiveTime and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<table>
<thead>
<tr>
<th>Information System Security Officer or System Owner</th>
<th>Information Technology Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Teresa Coppolino</td>
<td>Name: Ammar Ahmad</td>
</tr>
<tr>
<td>Office: OFMS/CSC</td>
<td>Office: OFMS/CSC</td>
</tr>
<tr>
<td>Phone: 301-355-5501</td>
<td>Phone: 301-355-5601</td>
</tr>
<tr>
<td>Email: <a href="mailto:tcoppolino@doc.gov">tcoppolino@doc.gov</a></td>
<td>Email: <a href="mailto:aahmad@doc.gov">aahmad@doc.gov</a></td>
</tr>
</tbody>
</table>

Signature: TERESA COPPOLINO  
Digitally signed by TERESA COPPOLINO  
Date: 2021.05.07 16:41:53 -04'00'

Signature: Ammar Ahmad  
Digitally signed by Ammar Ahmad  
Date: 2021.05.06 12:43:53 -04'00'

<table>
<thead>
<tr>
<th>Privacy Act Officer</th>
<th>Authorizing Official</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Tahira Murphy</td>
<td>Name: Stephen Kunze</td>
</tr>
<tr>
<td>Phone: 202-482-8075</td>
<td>Phone: 202-482-3709</td>
</tr>
<tr>
<td>Email: <a href="mailto:tmurphy2@doc.gov">tmurphy2@doc.gov</a></td>
<td>Email: <a href="mailto:skunze@doc.gov">skunze@doc.gov</a></td>
</tr>
</tbody>
</table>

Signature: TAHIRA MURPHY  
Digitally signed by TAHIRA MURPHY  
Date: 2021.06.30 08:52:06 -04'00'

Signature: STEPHEN KUNZE  
Digitally signed by STEPHEN KUNZE  
Date: 2021.05.10 17:55:08 -04'00'

<table>
<thead>
<tr>
<th>Bureau Chief Privacy Officer</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Maria Dumas</td>
<td></td>
</tr>
<tr>
<td>Office: Office of Privacy and Open Government</td>
<td></td>
</tr>
<tr>
<td>Phone: 202-482-5153</td>
<td></td>
</tr>
<tr>
<td>Email: <a href="mailto:mdumas@doc.gov">mdumas@doc.gov</a></td>
<td></td>
</tr>
</tbody>
</table>

Signature: MARIA STANTON-DUMAS  
Digitally signed by MARIA STANTON-DUMAS  
Date: 2021.07.02 17:43:53 -04'00'

Date signed: ________________________________