PRIVACY IMPACT ASSESSMENT

Diplomatic Security Business Services Suite (DS BSS)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) **Date of completion of this PIA:** 04/13/2021

(b) **Name of system:** DS Business Services Suite

(c) **System acronym:** DS BSS

(d) **Bureau**: Diplomatic Security (DS)

(e) **iMatrix Asset ID Number:** 104984

(f) **Child systems (if applicable) iMatrix Asset ID Number:** N/A

(g) **Reason for performing PIA:**

☒ New system
☐ Significant modification to an existing system
☐ To update existing pia for a triennial security reauthorization

(h) **Explanation of modification (if applicable):**

N/A

3. General Information

(a) **Does the system have a completed and submitted data types document in Xacta?**

☒ Yes
☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) **Is this system undergoing an Assessment and Authorization (A&A)?**

☒ Yes
☐ No

If yes, has the privacy questionnaire in Xacta been completed?
☒ Yes
☐ No

(c) **Describe the purpose of the system:**

The DS Business Services Suite (DS BSS) is a commercial reporting platform with a host of applications that provides shared business services to multiple DS applications. DS BSS is considered part of the DS Chief Technology Officer (DS/CTO) Service Delivery Model (SDM). Data reporting, data discovery, electronic data exchange, and business intelligence capabilities are delivered with DS BSS, which is a central component used to meet many DS stakeholder requirements for data aggregation, statistical reporting, system connection, and ad-hoc data discovery. At this time, the reporting platform consists of: (1) BizTalk; (2) Business Objects (BO); (3) Power Business Intelligence (Power BI); and (4) Autonomy. Future integrations will be discussed in subsequent privacy impact assessments.

(d) **Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:**

The DS BSS platform does not collect PII; however, it maintains an array of PII. DS BSS is a reporting platform that provides data reporting, data discovery, electronic data exchange, and business intelligence capabilities.

PII is collected, used, maintained, and/or disseminated at the application level; therefore, PII is discussed in each application's PIA. Examples of PII maintained by DS BSS are listed below:

- Name;
- Personal Phone Number;
- Personal email Address;
- Personal Address;
- Full Social Security Number;
- Passport Number;
- National ID (for Non-US Citizens);
- Date of Birth;
- Place of Birth;
- Citizenship;
- Educational;
- Financial Information;
- Personnel/Employment;
- Mother's Maiden Name;
- Legal;
- Biometric Records (photographs and fingerprints);

- Business Contact Work Email;
- Business Contact Work Phone Number;
- Business Contact Work Address.

The following applications reside on the DS BSS platform and all PII that resides within those applications is discussed in each application's PIA:

- Diplomatic Security General Support System Platform as a Service (DS G-PaaS)
- Personnel Accounting Integrated Reporting System (PAIRS)
- Computerized Maintenance Management System (CMMS)
- Post Emergency Guidance and Authoring System (PEGSYS)
- Regional Security Office Local Vetting (RESOLVE)
- Protective Liaison Case Tracking System (POLCATS)
- Investigative Management System – Unclassified (IMS-U)
- Security Incident Management and Analysis II (SIMAS II)
- Diplomatic Security Business Process Management Suite (DS BPMS)
- Identity Management System (IDMS)
- Diplomatic Security Planning Structure (DSPS)
- Diplomatic Security Audio Bridge (DSAB)
- Diplomatic Security – Employee Tracker (DS-ET)

(e) **What are the specific legal authorities and/or agreements that allow the information to be collected?**

- Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. § 4802, as amended; and
- Foreign Assistance Act, 22 U.S.C. § 2349aa et. seq.

DS business owners and program managers are responsible for identifying the proper authorities for each application that uses DS BSS, therefore, each application PIA will discuss the appropriate legal authorities for its particular PII collection.

(f) **Is the information searchable by a personal identifier (e.g., name or Social Security Number, etc.)?**

☒ Yes, provide:

- SORN Name and Number: STATE-36, Security Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

- SORN Name and Number: STATE-40, Employee Contact Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): April 24, 2018

☐ No, Explain How the Information is Retrieved Without a Personal Identifier.

(g) **Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?** ☐Yes ☒ No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) **Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?** ☐Yes ☒ No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

The DS BSS platform does not collect PII; however, it maintains an array of PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, the records retention schedule is discussed in each application's PIA.

If yes, provide (consolidate as much as possible):
- Schedule Number (e.g., (XX-587-XX-XXX)):
- Disposition Authority Number:
- Length of time the information is retained in the system:
- Type of information retained in the system:

4. Characterization of the Information

(a) **What entities below are the original sources of the information in the system? Please check all that apply.**

☒ Members of the Public
☒ U.S. Government Employees/Contractor Employees
☒ Other (People who are not U.S. Citizens or LPRs)

(b) **On what other entities above is PII maintained in the system?**

☐ Members of the Public
☐ U.S. Government Employees/Contractor Employees
☐ Other
☒ N/A

(c) **If the system contains Social Security Numbers (SSNs), is the collection necessary?**

☐Yes ☐No ☒ N/A

The DS BSS platform does not collect PII; however, it maintains an array of PII. Social Security numbers are collected, used, maintained, and/or disseminated at the application

level; therefore, the necessity of the collection of Social Security numbers is discussed in each relevant application's PIA.

- If yes, under what authorization?

(d) **How is the PII collected?**

The DS BSS platform does not collect PII; however, it maintains an array of PII. PII is collected at the application level; therefore, the method of collection is discussed in each application's PIA.

(e) **Where is the information housed?**

☒ Department-owned equipment
☐ FedRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

(f) **What process is used to determine if the PII is accurate?**

The DS BSS platform does not collect PII; however, it maintains an array of PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, the process used to determine if the PII is accurate is discussed in each application's PIA.

(g) **Is the information current? If so, what steps or procedures are taken to ensure it remains current?**

The DS BSS platform does not collect PII; however, it maintains an array of PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses the processes used to determine whether the PII is current, and what steps and procedures are taken to ensure it remains current.

(h) **Does the system use information from commercial sources? Is the information publicly available?**

No. Commercial data are not used and the information is not publicly available.

(i) **How was the minimization of PII in the system considered?**

The DS BSS platform does not collect PII; however, it maintains an array of PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, the minimization of PII use is discussed in each application's PIA.

5. Use of Information

(a) **What is/are the intended use(s) for the PII?**

DS BSS utilizes PII within it for the creation of reports requested by DS applications. Application systems process data based upon the purpose and function of the application. Data fall into several categories such as law enforcement data, inventory data, personnel records, etc.

PII is collected, used, maintained, and/or disseminated at the application level; therefore, the intended use for the PII are discussed in each application's PIA.

(b) **Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?**

Yes, the use of PII is relevant to the purpose for which the DS BSS platform was designed. Additionally, PII at the application level is relevant to the purpose for which each application was designed; therefore the purposes for the use of the PII is discussed in each application's PIA.

(c) **Does the system analyze the PII stored in it?** ☐Yes ☒ No

If yes:
(1) What types of methods are used to analyze the PII?
(2) Does the analysis result in new information?
(3) Will the new information be placed in the individual's record? ☐Yes ☐No
(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) **If the system will use test data, will it include real PII?**

☐Yes ☐No ☒ N/A

If yes, please provide additional details.

6. Sharing of PII

(a) **With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.**

Internal:
The DS BSS platform does not share any PII internally with any other DS system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses with whom the PII may be shared internally.

External:
The DS BSS platform does not share any PII externally with any other system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses with whom the PII will be shared externally.

(b) **What information will be shared?**

Internal:
The DS BSS platform does not share any PII internally with any other DS system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses what PII will be shared internally.

External:
The DSS BSS platform does not share any PII externally with any other system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses what PII will be shared externally.

(c) **What is the purpose for sharing the information?**

Internal:
The DS BSS platform does not share any PII internally with any other DS system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses its purpose for sharing the PII internally.

External:
The DS BSS platform does not share any PII externally with any other system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application PIA discusses the purpose for sharing the PII shared externally.

(d) **The information to be shared is transmitted or disclosed by what methods?**

Internal:
The DS BSS platform does not share any PII internally with any other DS system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses its method of transmission for PII shared internally.

External:
The DS BSS platform does not share any PII externally with any other system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses the method of transmission for PII shared externally.

(e) **What safeguards are in place for each internal or external sharing arrangement?**

Internal:
The DS BSS platform does not share any PII internally with any other DS system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses its internal sharing arrangement safeguards.

External:
The DS BSS platform does not share any PII externally with any other system. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses its external sharing arrangement safeguards.

7. Redress and Notification

(a) **Is notice provided to the record subject prior to the collection of his or her information?**

The DS BSS platform does not collect PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses whether a notice is provided to the record subject prior to the collection of his or her PII.

(b) **Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?**

☐Yes ☒ No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

The DS BSS platform does not collect PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discuss discusses whether the record subject is allowed to provide consent or not.

(c) **What procedures allow record subjects to gain access to their information?**

The DS BSS platform does not collect PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses what procedures allow record subjects to gain access to their PII.

(d) **Are procedures in place to allow a record subject to correct inaccurate or erroneous information?**

☐Yes ☒ No

If yes, explain the procedures.

If no, explain why not.

The DS BSS platform does not collect PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses what procedures are in place to allow a record subject to correct inaccurate or erroneous PII.

(e) **By what means are record subjects notified of the procedures to correct their information?**

The DS BSS platform does not collect PII. PII is collected, used, maintained, and/or disseminated at the application level; therefore, each application's PIA discusses the procedures for record subjects to correct their PII.

8. Security Controls

(a) **How is all of the information in the system secured?**

The PII in the DS BSS platform is secured by inherited security controls from the DS G-PaaS system boundary and authorization. The DS BSS platform is also secured by the use of the Microsoft SQL databases and their role-based access controls (RBAC) security functions and responsibilities.

The DS ISSO is responsible for the security management of the DS BSS platform. The ISSO works with the DS/CTO/ASB Team to ensure that continuous monitoring is in place for DS BSS and compliance with Department security requirements.

The Splunk and BelManage security monitoring tools are in place. The Splunk monitoring tool is used to monitor baseline configuration settings for the servers, and BelManage is used to monitor the IT inventory. Automated vulnerability scans are conducted for the DS BSS databases, to ensure compliance with Department continuous monitoring requirements.

Security controls are tailored and configured to protect PII maintained within each application; therefore, each application's PIA discusses how that application is secured.

(b) **Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).**

Only authorized, cleared DoS direct hire and contractor employees are allowed access to the DS BSS servers, databases, and platform.

The following three (3) roles have been created to provide access to DS BSS and the PII contained within DS BSS:

- System Administrators: The System Administrators are the only users authorized to access DS BSS servers with privileged access for purposes of troubleshooting and performing routine maintenance.
- Database Administrators: The Database Administrators are the only users authorized to access DS BSS databases with privileged access for purposes of troubleshooting and performing routine maintenance.
- Application Administrators: The Application Administrators are the only users authorized to administer the DS BSS platform and its users.

Each application's PIA discusses the different roles that have been created to provide access to it and the PII it contains.

(c) **Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.**

RBAC controls are in place for the DS BSS platform for System Administrators, Database Administrators, and Application Administrators who have an "official" need to access the PII in their work capacity.

Access controls are configured and are in place at each application level. The procedures established to limit system and data access to only those individuals who have an "official" need to access the PII in their work capacity are discussed in each application's PIA.

(d) **How is access to data in the system determined for each role identified above?**

Access to the DS BSS platform for System Administrators, Database Administrators, and Application Administrators is determined by the DS/CTO/ASB Branch Chief and is based upon approved RBAC roles and permissions.

Access to PII maintained at the application level will be discussed in each application's PIA.

(e) **What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?**

The PII in the DS BSS platform is monitored, recorded, and audited by the inherited security controls from the DS G-PaaS system boundary and authorization. The DS BSS platform also monitors, records, and audits PII in order to prevent the misuse of the PII.

PII stored in the MS SQL database server (discussed in 8(a)) resides behind a DS-managed NSX firewall that limits access to the reporting platform and monitors server event logs. In addition, the Splunk monitoring tool is used to monitor access and changes to all DS BSS servers, and the EMC Avamar data backup recovery tool is used to save backups and to recover lost data if needed.

Safeguards to protect PII maintained at the application level are configured for each application and will be discussed in each application's PIA.

(f) **Are procedures, controls or responsibilities regarding access to data in the system documented?**

☒ Yes ☐ No

(g) **Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.**

The DS BSS platform Administrators, System Administrators, and Database Administrators must complete the following:

- Must attend a security briefing prior to receiving access to DoS networks and receiving a PIV card for building access. This briefing is sponsored by DS Security Infrastructure, Office of Information Security (DS/SI/IS) and includes a discussion of the Privacy Act of 1974.
- Must take PS800 'Cybersecurity Awareness', which has a privacy component, and quiz prior to receiving access to a DoS network. This briefing is an annual requirement.
- Must take PA318 'Protecting Personally Identifiable Information' within 90 days of their start date, and every two (2) years thereafter.
- Must review and sign a 'Security Briefing for DS Network and Application Users', which has a privacy component before they are given access to the DoS networks.
- Must follow the DoS-mandated Security Awareness Program that is in-place for IT professionals. In order to gain access as an Administrator, an individual must attend the 'Information Assurance Training for System and Security Administration' course, which has a privacy component, and obtain a certificate of completion.