G-PaaS PIA

1. Contact Information

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

2. System Information

(a) Name of system: Diplomatic Security General Support System Platform as a Service

(b) Bureau: Diplomatic Security

(c) System acronym: DS G-PaaS

(d) iMatrix Asset ID Number: 277882

(e) Reason for performing PIA:

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
G-PaaS is currently undergoing A&A activities. The system is in "Step 4: Security Assessment" of the A&A process. The estimated scheduled completion date for authorization is July 2020.

(c) Describe the purpose of the system:
The Diplomatic Security General Support System Platform as a Service (DS G-PaaS), supports the Bureau of Diplomatic Security (DS) mission requirements as an approach to organizing and managing DS baseline IT assets. The G-PaaS system is also a general support system that provides the core functional platform components grouped together to provide baseline configuration and maintenance for DS applications under the same direct management control.

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

The G-PaaS is a general support system. PII stored in the database servers within the G-PaaS boundary, but PII is collected, processed, maintained, and/or disseminated at the application level; therefore collection of PII is discussed in the PIAs for applications that reside on G-PaaS. G-PaaS will be treated as the overarching platform for organizing and managing baseline IT assets and virtual systems (applications) provided by the Department Enterprise Server Operation Center (ESOC); therefore, DS is unable to enumerate all of the applications that will reside on G-PaaS and all of the PII that will reside within those applications supported by it. However, a few examples of PII that may be maintained in those applications are listed below:

- Names
- Social Security Number
- Birthdates
- Phone number(s)
- Email address
- Home address
- Business address
- Business email
- Images or Biometrics IDs

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

For G-PaaS, the legal authority for the collection of information is the same as that which established the Bureau of Diplomatic Security: The Omnibus Diplomatic Security and Anti-terrorism Act of 1986 (Pub. L. 99-399; 22 U.S.C. 4801, et seq. (1986)) as amended. This legislation is cited in 12 Foreign Affairs Manual (FAM) 012, Legal Authorities.

DS business owners and program managers are responsible for identifying the proper authorities for the applications that use the G-PaaS infrastructure. Therefore, each application PIA will discuss the appropriate authorities for its particular PII collection.

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

☐Yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

☒No, explain how the information is retrieved without a personal identifier.

The personal identifier is retrieved at application level. G-PaaS is a general support system and PII is not retrieved from it. Each application PIA will discuss whether or not information is searchable via 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 Division 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 .)
PII stored within the G-PaaS boundary or G-PaaS databases is determined at the application level. As PII is maintained at the application level, each application PIA will indicate the records retention schedule for its particular collection of PII.

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) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No - The G-PaaS system does not collect SSNs.

- If yes, under what authorization?

(c) How is the information collected?
PII is collected at the application level and detailed information about the collection of this data is covered in each application's PIA.

(d) 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.

(e) What process is used to determine if the information is accurate?
DS G-PaaS does not use PII, but provides the infrastructure for other DS applications that are responsible for the PII. The applications that collect PII using the G-PaaS

infrastructure are covered by their own separate PIAs. Any information regarding the accuracy of information will be discussed in individual application PIAs.

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

DS G-PaaS does not use PII, but provides the infrastructure for other DS applications that are responsible for the PII. The applications that collect PII using the G-PaaS infrastructure are covered by their own separate PIAs. Any information regarding the accuracy of information will be discussed in individual application PIAs.

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

No. Commercial data is not used and the data collected is not available to the public.

(h) Is notice provided to the individual prior to the collection of his or her information?

DS business owners and program managers are responsible for the proper collection, use, and maintenance of PII data for specific applications that use the G-PaaS infrastructure. The applications that collect, maintain, and store PII using the G-PaaS infrastructure are covered by their own separate PIAs and notice provided to subjects of PII collection will be addressed in those PIAs.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

DS business owners and program managers are responsible for the proper collection, use, and maintenance of PII for specific applications that use the G-PaaS infrastructure. The applications that collect, maintain, and store PII using the G-PaaS infrastructure are covered by their own separate PIAs, which will discuss whether or not individuals are provided the opportunity to decline to provide the PII or to consent to particular uses of the PII they collect/maintain.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

This question does not apply to the G-PaaS. G-PaaS functions as an IT infrastructure for DS applications. PII data is not managed or maintained at the G-PaaS level, but at the application level, therefore, this will be addressed in individual application PIAs.

5. Use of information

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

DS G-PaaS does not use PII, but provides the infrastructure for other DS applications that are responsible for the PII. The applications that collect PII using the G-PaaS infrastructure are covered by their own separate PIAs. The intended uses of information will be discussed at the application level within individual application PIAs.

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

DS G-PaaS does not use PII, but provides the infrastructure for other DS applications that are responsible for the PII. The applications that collect PII using the G-PaaS infrastructure are covered by their own separate PIAs, which discuss the relevance of PII they maintain.

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

If yes:

(1) What types of methods are used to analyze the information?

(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

6. Sharing of Information

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

DS business owners and program managers are responsible for the proper collection, use, and maintenance of PII data for specific applications that use the G-PaaS infrastructure. and at no time is PII in G-PaaS shared internally or externally. Any internal or external sharing of PII that occurs at the application level is discussed in the respective application's PIA.

(b) What information will be shared?

Not applicable as PII in G-PaaS is not shared internally or externally. Any internal or external sharing of PII that occurs at the application level is discussed in the respective application's PIA.

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

Not applicable as PII in G-PaaS is not shared internally or externally. . Any internal or external sharing of PII that occurs at the application level is discussed in the respective application's PIA.

The information to be shared is transmitted or disclosed by what methods?

Not applicable as PII in G-PaaS is not shared internally or externally. Any internal or external sharing of PII that occurs at the application level is discussed in the respective application's PIA.

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

Not applicable as PII in G-PaaS is not shared internally or externally. Any internal or external sharing of PII that occurs at the application level is discussed in the respective application's PIA.

(e) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Not applicable as PII in G-PaaS is not shared internally or externally. Any internal or external sharing of PII that occurs at the application level is discussed in the respective application's PIA.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

DS G-PaaS does not use PII, but provides the infrastructure for other DS applications that are responsible for the PII. DS system business owners and program managers are responsible for the proper collection, use and maintenance of PII in DS applications that use the G-PaaS infrastructure. The applications that collect, maintain and store PII using the G-PaaS infrastructure are covered by their own separate PIAs, which will discuss this.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

DS G-PaaS does not use PII, but provides the infrastructure for other DS applications that are responsible for the PII. DS system business owners and program managers are responsible for the proper collection, use and maintenance of PII in DS applications that use the G-PaaS infrastructure. The applications that collect, maintain and store PII using the G-PaaS infrastructure are covered by their own separate PIAs. Procedures for correcting inaccurate or erroneous information will be documented in individual application system PIAs.

(c) By what means are individuals notified of the procedures to correct their information?

DS system business owners and program managers are responsible for the proper collection, use and maintenance of PII in DS applications that use the G-PaaS infrastructure. The applications that collect, maintain and store PII using the G-PaaS infrastructure are covered by their own separate PIAs. Procedures to correct data will be listed in the applicable PIAs for applications.

8. Security Controls

(a) How is the information in the system secured?

PII stored in the G-PaaS database servers and is collected, processed, maintained, and/or disseminated at the application level. At the G-PaaS level, 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 software and hardware inventory of the servers. Automated vulnerability scans are conducted for the databases to ensure compliance with Department continuous monitoring requirements. At the application level, security controls to protect PII are configured for individual applications and will be discussed in the PIA for each application that resides on G-PaaS. The G-PaaS monitoring controls are inherited at the application level as well.

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

G-PaaS is the platform for DS applications. Least privilege is in place for system administrators (SAs) and database administrators (DBAs). Application specific controls are configured at the application-level for DS applications and will be addressed in applicable system security plans. However, the application administrators are not members of the SA and/or DBA groups They have no local system access privileges, and only have permissions to administer the application and its users once it has been installed. Application users are provisioned by application administrators and assigned to user groups defined within the application that map to their functional organizational role. This ensures that least privilege and separation of duties are enforced within the

application. Application users also do not have local system access privileges. Application database users IDs are created so that only the application ID interacts directly with the database, not users. System administrators (SAs) and database administrators (DBAs) are not provisioned as application users to ensure that least privilege and separation of duties are enforced within the application. SAs are responsible for configuring and maintaining the baseline operational security controls for the operating systems and virtual firewalls. The DBA is responsible for configuring and maintaining baseline operational security controls for the Oracle and MS SQL databases.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

PII stored in the G-PaaS database servers resides behind DS managed NSX firewalls that limit access to the infrastructure and monitor server event logs. In addition, the Splunk monitoring tool, is used to monitor access and changes to all system servers, and the EMC Avamar data backup recovery tool is used to save backups and to recover lost data if needed. At the application level, safeguards to protect PII are configured for individual applications and will be discussed in the PIA for each application that resides on G-PaaS.

(d) Explain the privacy training provided to authorized users of the system.

Department users are required to attend a security briefing before access to Department systems is granted. This briefing also includes a privacy orientation. Users are also required to complete the Cybersecurity Awareness Training course, which contains a module on privacy, on an annual basis, and must acknowledge Department policies (including Department privacy policies) by signing user agreements. System administrators and privileged users are required to complete a separate security awareness briefing provided by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding and Rules of Behavior statement. The Protecting PII (PA459) course is required for all Civil Service, Foreign Service and Locally Employed Staff that handle PII.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

Authentication is handled by Single Sign-On (SSO) procedure, information access is controlled by manual owner permission and an Active Security List at the G-PaaS level. Non-production uses (e.g., testing, training) of production data are limited by administrative controls. In addition, the Department uses an array of configuration

auditing and vulnerability scanning tools and techniques to periodically monitor G-PaaS servers for changes to the DOS mandated security controls. At the application level, security controls to protect PII are configured for individual applications and will be discussed in the PIA for each application that resides on G-PaaS.

(f) How were the security measures above influenced by the type of information collected?
Data files are categorized at the Sensitive but Unclassified level. The appropriate NIST SP 800-53 controls are in place based upon the FIPS 199 risk categorization of data. All data is encrypted and only authorized access is granted at the application level. Within the G-PaaS environment, database and system administrators have access to data based upon system privileges and roles. As a result, monitoring tools are used to ensure the security of the data. See Question and Answer 8 (c). Only database and system administrators are allowed to access data at the G-PaaS level and that access is based upon management of the configuration settings in place for the servers.

How each application's applicable security measures were influenced by the type of PII it maintains will be discussed in its PIA.

9. Data Access

(a) Who has access to data in the system?
Only authorized system and database administrators have access to the data in the G-PaaS databases (including PII) at the G-PaaS level. Access to PII maintained at the application level will be discussed in separate application PIAs.

(b) How is access to data in the system determined?
Access to G-PaaS is determined by the DS/CTO/ASB Branch Chief and is based upon approved roles and permissions. Only system and database administrators have access to the servers within the G-PaaS boundary. Access to PII maintained at the application level will be discussed in the PIA for each application which resides on G-PaaS.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
No. Role-based access controls are in place for G-PaaS. Only authorized system and database administrators have access to G-PaaS servers. They are responsible for the baseline configuration of the operating system and database servers within the G-PaaS boundary. Access controls in place for individual applications will be discussed in PIAs for each application. General applications users do not have access to the G-PaaS infrastructure.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

For PII within the G-PaaS database servers, access controls are in place for the back-end Oracle and MS SQL 2016 database systems. Access is based on role-based permissions configured for “least privilege”, which establishes separation of duties. Only system administrators and database administrators are authorized to access G-PaaS for the management and maintenance of Department baseline configuration settings. Authentication is established via Windows Authentication using single sign-on via the OpenNet general support system, and auditing is performed by the Splunk monitoring tool to monitor user actions for Windows, Oracle and MS SQL Server. Controls to prevent the misuse of PII by users having access to PII maintained at the application level will be discussed in the PIA for each application residing on G-PaaS.