

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- (a) Date PIA was completed: April 15, 2009
- (b) Name of system: Eagle Portal
- (c) System acronym: DS EAGLE
- (d) IT Asset Baseline (ITAB) number: 725
- (e) System description (Briefly describe scope, purpose, and major functions):

DS Eagle is the collection of software, hardware, standard reference tables, and standard operating procedures that provide the common services that fully and cost-effectively support the development, deployment, operation, and maintenance of the Information Technology (IT) applications necessary for the Bureau to successfully meet its mission goals and objectives.

DS Eagle provides a platform that supports applications which are vital to DS's worldwide mission. This platform provides a central repository and management tools for user information, roles and credentials that can be integrated with any application hosted on the platform.

- (f) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security re-certification
- (g) Explanation of modification (if applicable): Format modification
- (h) Date of previous PIA (if applicable): January 2008

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The type of data/information captured is relative to the account management aspects of the DS Eagle platform. The platform provides account management services to the applications hosted. Since each application hosted on this platform has a PIA that

addresses its data specifically, this PIA addresses only the data elements common to all hosted applications and otherwise not addressed by their respective PIAs.

A sample of the common information that could be collected in regards to a particular case, in as follows:

- First Name;
- Last Name;
- Email address;
- Office Title;
- Office Phone

b. How is the information collected?

The primary source of the data collected by DS Eagle is from the individual requesting access to an application hosted on the Eagle platform. This information can be collected via paper or web-based forms.

c. Why is the information collected and maintained?

The information within DS Eagle is collected and maintained for the purpose of supporting the applications hosted on the DS Eagle platform.

d. How will the information be checked for accuracy?

The individual providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by DS include, among other things, maintaining the system as a live feed, allowing the information to be updated/edited at any time, and cross referencing information with other source systems for accuracy.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to DS Eagle, are as follows:

- Pub.L. 99-399(Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended);
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

DS Eagle collects the minimum amount of personally identifiable information necessary to provide a central repository and management tools for user information, roles and credentials that can be integrated with any application hosted on the platform.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

DS Eagle provides a platform that supports applications which are vital to DS's worldwide mission. This platform provides a central repository and management tools for user information, roles and credentials that can be integrated with any application hosted on the platform.

b. What types of methods are used to analyze the data? What new information may be produced?

No analysis of the common data is performed. However, the applications supported may perform their own analysis as defined within their respective PIA's. Furthermore, no new information is derived.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

The system does not use any commercial information, publicly available information, or information from other Federal agency databases.

d. Is the system a contractor used and owned system?

DS Eagle is a Government owned system which was primarily designed and developed by contractors. All contractors have abided to regulatory guidelines and have signed and follow the DoS Rules of Behavior.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

DS Eagle performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

DS Eagle is a government owned system supported by contract employees, who support U.S. Government employees in their maintenance of the system. Both contractors and government employees who support and use DS Eagle are subjected to a background investigation of the files of certain U.S. Government agencies (e.g., criminal law

enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

DS Eagle collects and maintains first and last names, office titles, and phone numbers. There are inherent risks associated with these types of information. In an attempt to mitigate these risks the Department of State has implemented numerous management, operational, and technical security controls in order to protect the information in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software) and audit reports.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information collected by DS Eagle is shared across the DoS on a "need-to-know" basis in support of DS's worldwide investigative mission.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

In order to access DS Eagle users must first authenticate to the system, which utilizes ID and password authentication. System authentication is based upon role-based control and session management. An end user is only granted access rights once he/she has authenticated to DS Eagle. All actions performed within the system are audited by controls configured for the operating system and database.

Moreover, numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

It is possible for an employee working for the Department of State to use his or her access to this information to retrieve contact information on an individual and use this information in an unauthorized manner. In order to mitigate this risk all Department employees are required to undergo computer security and privacy awareness training prior to accessing OpenNet, through which the information is shared, and must complete refresher training yearly in order to retain access.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

DS Eagle does not share information with any external organizations.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

No information from DS Eagle is shared with other external organizations.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Not Applicable.

8. Notice

The system:

- Contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit www.state.gov/m/a/ips/c25533.htm for list of all published systems):

STATE-36

- Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-36.

b. Do individuals have the opportunity and/or right to decline to provide information?

Before divulging information via the telephone (Land-Line, Mobile, or Internet), the individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also

described in the System of Records Notice titled STATE-36. If the user does not provide the necessary information, the individual will not be granted access to DS Eagle.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No, the system would not be able to process the application without all the required information.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

DS Eagle contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the data in the system is on a "need-to-know" basis and/or under routine use criteria as explained in STATE-36. Criteria, procedures, controls, and responsibilities regarding access are all documented.

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is

displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Diplomatic Security uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the DS Eagle components, for changes to the DoS mandated security controls.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. DS Eagle has been designed to minimize risk to privacy data. Please refer to 11(b) for further information.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The next C&A for DS Eagle is scheduled to be completed in September 2009.