



Privacy Impact Assessment
Diplomatic Security Business
Process Management System
(DS BPMS)

UNIQUE PROJECT IDENTIFIER ITAB
NUMBER: 4162

1. Contact Information

Department of State Privacy Coordinator

Sheryl Walter
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- (a) Date PIA was completed: January 17, 2014
- (b) Name of system: Diplomatic Security Business Process Management System
- (c) System acronym: DS BPMS
- (d) IT Asset Baseline (ITAB) number: 4162
- (e) System description (Briefly describe scope, purpose, and major functions):

The DS BPMS application is a web-based work flow management tool developed by the Department of State (DoS) Bureau of Diplomatic Security (DS) Office of the Chief Technology Officer (DS/EX/CTO). It is an implementation of the Metastorm Business Process Management (BPM) commercial off-the-shelf (COTS) software product. DS BPMS is designed to support rapid deployment and customization of human and system-based processes within and across the DS organization, including the design, automation, and management of multiple processes with an emphasis on enabling real-time, roundtrip process improvement through a combination of modeling, integration, execution, and simulation technologies, all arranged through a single interface.

Through the use of the seven separate workflows within DS BPMS, users can request access to a wide range of DS resources such as networks, applications, information, and hardware. These work flows are Network Access Request (NAR), Portable Device Tracking System (PDTs), Purchase Request and Ordering Process System (PROPS), High-Threat Integrated Tracking System (HITS), Computer Security Process Automation (CSPA), Recruitment System (RECRUIT), and Automated Badge Request (ABR).

Network Access Request (NAR) - supports DS/CTO/OPS management of requests for OpenNet, ClassNet, LAN, e-mail, distribution list, and/or mailbox access. DS Domestic transfers, changes and new requests are all handled by this system. NAR allows users to enter their own account requests online and receive routine updates on the status of their request.

Portable Device Tracking System (PDTs) – is a web-based inventory management and workflow system developed to effectively track and manage portable electronic devices. PDTs was built to better safeguard DS laptops by keeping track of who has them at all times.

Purchase Request and Ordering Process System (PROPS) – provides users the ability to submit technology requests to DS/CTO. This web-based system replaces the paper-based Support Request Form (SFR).

High-Threat Integrated Tracking System (HITS) - is the main support system utilized for collecting critical information on contractor personnel working under the Worldwide

Protective Services program. HITS provides the DS High Threat Protection (HTP) Division with the ability to access contractor information through OpenNet at State Annexes and Posts overseas.

Computer Security Process Automation (CSPA) – supports the office of Computer Security by automating the request, document review, and approval process for private/official residence OpenNet connectivity requests from embassy or domestic senior management.

Recruitment System (RECRUIT) – automates the DS Office of Recruitment, Examination and Employment (HR/REE) recruitment processes. RECRUIT automates the recruitment application submission, review, testing, and intake process.

Automated Badge Request (ABR) – automates the approval process for initial and renewal Requests for Building Pass Identification Card—currently involving the paper Form DS-1838—for DoS domestic employees, cleared and uncleared contractors, vendors, and press.

(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): A new PIA is required due to the addition of the new work flow ABR.

(h) Date of previous PIA (if applicable): August 22, 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?

NAR (The sources of this information are DS employees and contractors):

- Full Names;
- Social Security Number (SSN);
- Clearance;
- Email Address (Work);
- Phone Number (Work);
- Title;
- Employment Status, i.e., FTE, Contractor, PSC, etc.

PDTS (The sources of this information are DS employees and contractors):

- Full Names;

- Email Address;
- Phone Number (Work).

PROPS (The sources of this information are DS employees and contractors):

- Full Names;
- Phone Number (Work);
- Email Address (Work);
- Addresses (Work).

HITS (The source of this information is DS contractors only):

- Full Names;
- SSN;
- Date of Birth;
- Citizenship;
- Employment Information;
- Gender;
- Third Country National/Local National Identifier Number;
- Place of Birth;
- US Driver's License Information;
- Home of Record (Address);
- Phone Number;
- Passport Information;
- Educational Information;
- Work Experience;
- Clearance Information;
- Medical Information.

CSPA (The source of this information is department employees only):

- Full Names;
- Phone Number (Work/Home);
- Address (Home);
- Email (Professional).

RECRUIT (The sources of this information are private citizens who are potential DS employees):

- Name;
- Gender;
- Race;
- Place of Birth;
- Date of Birth;
- SSN;
- Address (Home/Work);
- Phone Number (Mobile/Home/Work);
- E-Mail Address (Personal/Professional);
- Educational History;
- Job Experience;
- Military Status;
- Citizenship;

- Spouse Information;
- Security Clearance Information.

ABR (The sources of this information are domestic DS employees, contractors, vendors, and press):

- Name;
- Date of Birth;
- Social Security or Employee's Unique ID Number;
- DOS E-mail Address;
- Citizenship;
- Dual Citizenship;
- Gender;
- Applicant Home Address;
- Employer Name;
- Employer Phone and Fax Numbers;
- Employer Address

b. How is the information collected?

Each application within DS BPMS has a web interface that allows the user to input the applicable information into a web-based form that is specific to that application.

The level of sensitivity of the unclassified information accessed, processed, stored, and transmitted on DS BPMS is sensitive but unclassified (SBU). DS BPMS processes privacy data as defined by the Privacy Act of 1974.

c. Why is the information collected and maintained?

NAR: The information in NAR is collected and maintained for the purpose of processing user network and account requests. The information collected is required to verify the clearance and need-to-know of the individual requesting access.

PDTS: The information in PDTS is collected and maintained for the purpose of issuing and tracking laptops. The information collected is required to keep an accurate hand receipt inventory of the issued devices.

PROPS: PROPS collects PII for the purpose of capturing purchase requirements, specifications, requestor information, government approval information, delivery requirements, and funding sources. It maintains a historical track of purchase requests to allow for tracking through delivery and development of reports.

HITS: The PII collected and maintained by HITS is used to vet, approve, and track personnel on the State Department's Worldwide Protective Services (WPS) program.

RECRUIT: The information in RECRUIT is collected and maintained for the purpose of screening applicants for possible employment within the Department of State.

ABR: The PII collected and maintained by ABR is used to process requests for Building Pass Identification Cards (Form DS-1838) for department employees, cleared and uncleared contractors, vendors, and press.

d. How will the information be checked for accuracy?

NAR: The end user is responsible for the accuracy of the information provided. The end user is generally the Branch Chief, Government Manager, or contractor manager requesting access to the network and DS applications for new DS employees, contractor employees, or an employee transferring to a new organization within DS. He/she is required to have knowledge of an employee's information and the DS network and application resources the employee needs to perform his/her official duties within DS. Field checks are incorporated into the user interface and the background database to ensure all data fields are completed correctly.

PDTS: The end user is responsible for the accuracy of the information provided. The end users are DS employees or contractor employees requesting the use of a government laptop. Field checks are incorporated into the user interface and the background database to ensure all data fields are completed correctly.

PROPS: The employee processing the PROPS requests confirms the accuracy of the information either verbally or through e-mail with the requestor or government manager.

HITS: HTP OPS Center and the Industrial Security Division (IND) personnel manually verify data, a number of automated system checks have been implemented to ensure accuracy and consistency during data entry, and CTO maintains a tool that will be used to periodically assess data accuracy.

RECRUIT: The agency or source 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 the DS/MGT/HRM analyst or surrogates.

ABR: For a new Building Pass Identification Card, the authorized requestor is responsible for entering all of the data for the applicant on the ABR badge request form. For a card renewal or a reissue of a lost or damaged card, the applicant enters the data in the applicant's portion of the online Form DS-1838; the authorized requestor then reviews and approves that information and completes the rest of the form, and submits it to ABR.

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

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 Antiterrorism 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.

Additional guidance can be found at the following:

- 12 FAM 200, Protection and Investigations (HITS, RECRUIT, ABR)
- 12 FAM 400, Post Operations (HITS, CSPA)
- 12 FAM 500, Information Security (NAR, PDTS, PROPS)
- 12 FAM 600, Information Security Technology (NAR, PDTS, PROPS, CSPA)

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

The primary risk is that the PII collected could somehow become available outside of DS BPMS. To mitigate this risk, PII for all DS BPMS applications is collected by means of web-based forms that are accessible only by users who are authenticated to the Department's unclassified OpenNet. Only authorized personnel who meet [12 FAM 621.1a](#) (below) are allowed access to OpenNet.

Per 12 FAM 621.1a, "The Department of State has established personnel security procedures to ensure that all personnel accessing Department automated information system (AIS) processing resources have:

- The required access levels and need-to-know;
- Appropriate supervision; and
- Knowledge of their AIS security responsibilities."

Thus, PII collected by the applications on the DS BPMS platform remains within the OpenNet domain and is not accessible by the public. In addition, the continuous monitoring processes and recertification requirements in place within the Department further ensure that data, including PII, contained within DS BPMS is not compromised.

4. Uses of the Information

a. Describe all uses of the information.

NAR: The DS User Network and Application Account Request information is the initial component of DS BPMS. The names of individuals and social security numbers are used to identify end users. The clearance level is required to determine the access level for certain applications, such as Treasury Enforcement Communication System (TECS)/National Crime Information Center (NCIC), which require a clearance of Top Secret (TS). The phone number is required so individuals requiring an account can be located via phone in the Global Address List (GAL). The address provides the location of individuals requiring an account within DS.

A network or application account request web based form is used to collect all needed information/data required to establish the requested account(s). The submitted form is the initiating component of the account creation work flow process. Once the information is entered into the system, it undergoes an "approval" process that involves the following types of review before the account request is accepted and finalized:

1. Government Manager Review;
2. Security Review and/or DS/CTO/SMD/SEC Security Review;
3. ISSO Review; and
4. Operations in Process Review.

The information/data is not allowed to be used in a non-production environment (e.g., testing, training).

PDTS: The information in PDTS is collected and maintained for the purpose of issuing and tracking laptops. The information collected is required to keep an accurate hand receipt inventory of the issued devices.

PROPS: The information within PROPS is used to create reports for reference. Reports are generated on the category of purchases, purchase volume by office, type of purchases, and other ad hoc reports for management.

HITS: For each candidate there may be up to eight functions performed: create and approve biographical information (BIO), enter and confirm PII, designate affiliation, approve clearance, record employee actions, record training, and provide Letter of Authorization (LOA)/Common Access Card (CAC).

RECRUIT: The information is collected to determine whether the knowledge, skills, and abilities listed qualify a person to be hired. The PII will be used to verify citizenship and military service, to conduct an investigation and to determine employment suitability. The social security number is used to verify identify.

ABR: The information is collected and maintained solely for the purpose of issuing a new or renewal Building Pass Identification Card.

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

NAR: Analysis of the information/data is limited to reporting non-subject-based statistical information such as the number of assignments given to a Special Agent, dignitary assigned to, date of services, and a variety of standard reports.

Other analyses of the information include the number of submitted account requests, number of approved requests, the number of disapproved requests, modifications required before creation of an account, and the time associated with the various steps within the automated process. Of note is the amount of time it takes for the user to receive his/her account from the initial request submission.

PDTS: The information is analyzed by system users for accuracy. Comparison of tracking ID numbers is used to ensure that the correct individuals received the proper equipment.

PROPS: Analysis of the information within PROPS is done to support budget requests and future purchase requirements. No new information is generated.

HITS: HTP OPS and IND personnel are responsible for analyzing data to efficiently and effectively deploy personnel to support the Department of State Worldwide Protective Services program. HITS is a tracking system and there is no new information produced through analysis done by the system.

CSPA: The data is not analyzed. CSPA is used to streamline the approval process for OpenNet connectivity request from official residences, contractors, and other agencies.

RECRUIT: Analysis of the information is limited to non-subject-based statistical information, such as the applications in a particular status (i.e. received, working, approved, or mailed) on an aggregate cycle (i.e., Monthly, Quarterly, Yearly, etc.); number of inquires, number of responses, etc. Furthermore, no new information is derived.

ABR: The data is not analyzed. ABR is used to streamline the approval process for requests for a Building Pass Identification Card from domestic Department employees, cleared and uncleared contractors, vendors, and press.

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

DS BPMS does not use commercial information, publicly available information, or information from other Federal Agency databases.

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

DS BPMS is a government owned system which was primarily designed and developed by contractors. Users of DS BPMS are made up of FTE and contracting staff. All personnel are required to comply with regulatory guidelines and have signed and follow DS's 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.

Appropriate use is regulated by security controls in place for the application and by the System Rules of Behavior. Access controls are in place for the back-end Oracle database, which are based upon role-based permissions configured for "least privilege."

The review process establishes segregation of duties for the application. Authentication to the application is established via Windows Authentication using single sign-on. Once a user logs into OpenNet and is authenticated, the end user is granted access to the DS BPMS system. Because PII is present in the application, FIPS 140-2 encryption is in place for all sessions. Users are only allowed access to data required for their particular task. Validity checks for ensuring the proper information is submitted in the web forms are in place. The application does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

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, as follows:

Applica-tion	Section	Description	Disposition Schedule
NAR	A-11-038-12a	User Identification, Profiles, Authorizations, and Password Files - EXCLUDING records relating to electronic signatures (Systems requiring special	Temporary. Destroy/delete inactive file 6 (six) years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

Applica-tion	Section	Description	Disposition Schedule
		accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records.)	
NAR	A-11-038-12b	Ditto (Routine systems, i.e., those not covered by item 6a.)	Temporary. Delete/destroy when the Agency determines they are no longer needed for administrative, legal, audit, or other operational purposes
PDTS	A-11-017-04	Communications Equipment Tracking Files	Temporary. Destroy after items determined to be excess.
PROPS	A-11-038-09b(2)	IT Asset and Configuration Management Files	Temporary. Destroy/delete when 3 (three) years old or 1 (one) year after termination of system, whichever is sooner.
HITS	A-11-004-30	Contractor Security - Case File - Arrange by case	Cut off at the end of year in which security clearance expired. Destroy 5 years after the expiration of security clearance.
CSPA	A-11-031-01a–e	Computerized Management Maintenance System- CMMS	Temporary. Various
RECRUIT	A-11-004-31a & b	Department of State Personnel Security Case File (Applicant File)	Destroy when 5 years old. (each)
ABR	A-11-038-20	Building Pass Files	Temporary. Destroy when 1 (one) year old.

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

The PII remains protected within the restricted OpenNet domain for the duration of the time that it is retained. There are no identified risks associated with loss of records or unauthorized modification of data. Backup procedures are in place to protect the data, and all backups are stored off-site.

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?

NAR: Once the request is submitted via DS BPMS, the PII is not shared outside of DS.

PDTS: Once the information is input via DS BPMS, the PII is not shared outside of DS.

PROPS: Once the request is submitted via DS BPMS, the PII is not shared outside of DS.

HITS: Once the information is accessed via DS BPMS, the PII is not shared outside of DS.

CSPA: Once the request is submitted via DS BPMS, the PII is not shared outside of DS.

RECRUIT: Once the information is submitted via DS BPMS, the PII is not shared outside of DS.

ABR: Once the request is submitted via DS BPMS, the PII is not shared outside of DS.

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

Each application within the DS BPMS platform has an interface that allows the user to input information into a web-based form that is specific to an application. PII that is entered into DS BPMS is not transmitted or disclosed outside of DS BPMS, and is protected by the safeguards that protect DS BPMS within the accredited OpenNet environment. Access to OpenNet is strictly controlled in accordance with 12 FAM 621.1a.

There is no need to share PII from the applications within DS BPMS and thus no sharing arrangements exist.

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

PII that is entered into DS BPMS is not transmitted or disclosed outside of DS BPMS, and is protected by the safeguards that protect DS BPMS within the accredited OpenNet environment.

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?

Information in DS BPMS is not shared with any external organizations.

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

The information collected and maintained by DS BPMS is not shared with anyone outside the Department.

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

The information DS BPMS collects is not shared with any external organizations.

Unauthorized and/or unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and over an un-trusted communications link can also pose a significant risk. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with unauthorized external sharing and unintentional disclosure.

8. Notice

The system:

- Contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records:
STATE-31, Human Resource Records
STATE-36, Security Records
STATE-56, Network User Account Records
STATE-76, Personal Services Contractor Records
- 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, as described in the System of Records Notices STATE-36, Security Records, appears at the bottom of the screen on the web-based form for each application within DS BPMS. Also, STATE-36 and STATE-56 provide notice to the public about the type of collection of data in DS BPMS.

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

Yes. However, such action would prevent the individual from obtaining access to the system.

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?

Conditional consent is not applicable to the official purpose of the application.

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 system of records notice describes the purpose, uses, and authority of the collection of the personal information. The notice provided to the individual is reasonable and adequate.

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 BPMS 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 section 8 above, and in rules published at 22 CFR 171. 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.

If a request submitted to an application within DS BPMS is denied because information was entered incorrectly, the authorizing individual may allow the information to be corrected and the request to be resubmitted.

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?

The Business Owner DS/EX/CTO approves and authorizes use of the DS BPMS system. System accounts are maintained and reviewed on a regular basis. The following DoS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control

- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

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. Activity by authorized users is monitored, logged, and audited.

Access controls are in place for the back-end Oracle database, which are based on role-based permissions configured for “least privilege.” The review process establishes segregation of duties for the application. Authentication to the application is established via Windows Authentication using single sign-on. Once a user logs into OpenNet and is authenticated, the end user is granted access to the DS BPMS system. Because PII is present in the application, FIPS 140-2 encryption is in place for all sessions. Users are allowed access only to data required for their particular task. Validity checks for ensuring that the proper information is submitted in the web forms are in place. The application does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

The Oracle database resides in a protected domain. The domain is protected by a firewall configured to only receive requests from the web server. Only approved database administrators have direct access to the database. In addition, there are no external connections to the domain. Once a user no longer requires access to the application, the user’s account is disabled and then, after six months, is deleted. Application accounts are reviewed on a quarterly basis. Users not logging into the application for 90 days or more are automatically disabled.

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 BPMS components, for changes to the DoS mandated security controls.

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

Every DoS user must attend a security briefing which also includes privacy orientation prior to receiving access to DoS networks and access to DOS facilities. Each user must also complete Cybersecurity Awareness Training annually and sign a user access agreement form certifying that access is need for the performance of official duties.

System administrators and privileged users are required to complete a separate security awareness briefing given by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding and Rules of Behavior statement. Additionally, DS/CTO/SMD/SEC identifies key personnel within DS/CTO that need to attend the Department’s mandated Information Assurance training for system administrators.

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.

Because of controls that are in place that prevent unauthorized access and that allow only role-based access, risk caused by access issues is minimized. Additionally, audit logs are maintained and reviewed, and users are provided with security training before being given access to the system.

11. Technologies

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

No technologies commonly considered to elevate privacy risk are employed.

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

Because no technologies in DS BPMS elevate privacy concerns, no residual risk is expected.

12. Security

What is the security assessment and authorization (A&A) status of the system?

The A&A of DS BPMS was granted in September 2013.