Privacy Impact Assessment (PIA)

1. Contact Information

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: September 2, 2009

b. Name of system: Domestic Accounts Receivable Tracking System

c. System acronym: DARTS

d. IT Asset Baseline (ITAB) number: 271

e. System description (Briefly describe scope, purpose, and major functions):

DARTS version 5.5.8.2 has a full range of receivable management capabilities and interfaces with the Department's Global Financial Management System (GFMS) and the Department of the Treasury's Cross-Servicing Application. As of June 1, 2002, DARTS users have entered and managed over 42,173 receivables with original amounts totaling over $4.74 billion. The system has also processed over $3.48 billion in related collections from GFMS. DARTS provides flexibility for managing different types of receivables, a graphical user interface, and reporting capabilities that are not included in GFMS.

DARTS meets the requirements of the Federal Financial Management Improvement Act (FFMIA), the Government Performance and Results Act (GPRA), the Debt Collection Act, the Government Management Reform Act (GMRA), the Federal Managers' Financial Integrity Act (FMFIA), the National Security Agency (NSA), and other pertinent legislation. The mandated Intra-Governmental Revenue & Accounts Receivable Reconciliation Report was developed for Reconciliation of Accounts Receivable Records. DARTS also processes delinquent debtors for Credit Bureau Reporting.

DARTS is used by the Accounts Receivable Department and Working Capital Fund at the Global Financial Services Center (GFSC) in Charleston to enter and maintain domestic accounts receivable information for the Department of State (DOS). The primary functions of DARTS are:

- Receivable Maintenance. DARTS maintains 13 categories of receivables: Federal Government, Fiscal Irregularity, Foreign Government, Installation Agreement, Loan, Medical, Overpayment, Prepayment, Promissory Agreement, Salary Advance, Travel Advance, and Unused Ticket. Each receivable category requires different information and is governed by unique laws and regulations. In addition, to the categories, there is a Debtor Inquiry function, which enables the operator to get a list of all receivables for a particular debtor, along with a dollar total. This feature is used when a debtor inquires about a bill.

- Billing Cycle. The monthly cycle encompasses the aging of receivables (assessing charges, etc.) and their billing (generating notices). It processes receivables to determine refunds due, to be sent to a credit bureau or collection agency, etc.
- Manual Review. This function enables management actions such as salary and Internal Revenue Service (IRS) offsets collection agency and credit bureau submissions, write-offs, and closeouts. After the billing cycle, the user reviews receivables for further action, such as generating dunning notices.
- Interfaces. DARTS exchanges data with other systems through interfaces that are run at least monthly. These interfaces, subject to security restrictions, allow for transfer of data, thereby reducing manual data entry.
    - Receivable, collection, and reference table data are passed between DARTS and GFMS through a two-way interface. DARTS updates GFMS with receivable data, and GFMS returns any rejected receivables back to DARTS through a Rejected Interface. Collections originated in GFMS are transmitted to DARTS through an accepted interface.
    - DARTS interfaces with the Department of Treasury (DOT) Cross-Servicing application in support of the Debt Collection Improvement Act. This interface is one-way (output only) from DARTS in the form of a text file.

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):

h. Date of previous PIA (if applicable): 12/28/2006

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?

DARTS collects or maintains information from sources as listed below:

US Citizens:

- Name;
- Addresses;
- Social Security Number; and
- US passport number.

Civil and Foreign Service employees:

- Name;
- Addresses;
- Phone Number;
- Social Security Number;
- Employee identification number; and
- Bank account and routing number.

Vendor

- Corporate Name;
- Corporate Address;
- Phone Number;
- DUN;
- Tax identification number; and
- Bank account and routing number.

b. How is the information collected?

Consular Affairs at post use Form DS-3072 to collect information from U.S. citizens that request for financial assistance from the U.S. Government in order to return to the United States while aboard (repatriation). Consular Affairs at post prepares a cable identifying the need for the promissory agreement.

Advance travel to foreign post, travel advance receivables and vendor information are collected by Consolidated American Payroll Processing System (CAPPS). CAPPS interfaces with GFMS, which output the information for input into DARTS.

c. Why is the information collected and maintained?

Information is collected to identify individuals who have incurred a debt with DOS and to collect accounts receivables in accordance with Debt Collection Improvement Act (DCIA) of 1996.

d. How will the information be checked for accuracy?

Data generated through the DOS corporate applications are providing the level of accuracy equal to that of payroll on individuals. U.S. citizens' information is verified by the consular officer's for U.S. citizens abroad.

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

- 22 USC 2671
- 22 USC 3701

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

Risk are mitigated by collecting the absolute minimum PII required to satisfy the statutory purpose of this system and meet the mission of the Bureau.

4. Uses of the Information

a. Describe all uses of the information.

DARTS is the official domestic accounts receivable tracking system for the DOS. Under the DCIA of 1996, agencies are required to notify Treasury of delinquent debts over 180 days old so that Treasury may transfer legally enforceable delinquent debts for collection. The PII collected is reported to the Department of Treasury and used for the collection of those debts.

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

DARTS does not produce new information.

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

DARTS does not use data from commercial publicly available or from other Federal Agencies.

d. Is the system a contractor used and owned system? DARTS is owned and operated by Department of State.

There are contractors and DOS employees supporting the GFSC where DARTS is housed, operated and maintained. All contractors undergo an annual computer security briefing and Privacy Act briefing. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses.

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.

Personnel requiring access are required to submit a user agreement form which is approved by management personnel prior to access being granted. Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the access capabilities to those deemed necessary for specified job functions.

5. Retention

a. How long is information retained?

The retention period for payment, cash receipt and tax data is seven years.

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

Regular backups are performed and recovery procedures are in place for DARTS. All records containing personal information are maintained in secured file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention period they are immediately retired or destroyed in accordance with National Archive and Records Administration (NARA).

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?

DARTS shares reference table data with GFMS that allow for updates through a two-way interface between the systems. In addition DARTS reports to Consular Affairs passport office, list of individuals with delinquent payment that will be used to suspend the debtor's passport.

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

DARTS exchanges data described in 2e above with other systems through interfaces that are run at least monthly. These interfaces, subject to security restrictions, allow for transfer of data, thereby reducing manual data entry.

DARTS is accessed by authorized users by secure transmission methods permitted under DOS policy for handling and transmission of sensitive but unclassified information**.**

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

Internal sharing occurs only to registered users who are cleared government employees or contractors with work-related responsibility for DARTS. Risks to privacy are mitigated by providing only those reports associated with the persons permissions that are established by their supervisor and in conjunction with the information system security officer (ISSO).

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?

The following information may be shared:

- In support of the Debt Collection Act, list of all receivables for a particular debtor, the dollar total and the amount of refunds due can be shared with Credit Union or collection agency through Department of Treasury**.**
- Debt Collection and delinquent debts, in the form of an IRS Form 1099 is shared with the Internal Revenue Service for the purpose of debt collection.

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

DARTS interfaces with the Department of Treasury Cross-Servicing application. This interface is one-way (output only) from DARTS in the form of a text file. Information to IRS is provided on the IRS Form 1099.

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

Risks to privacy are mitigated by providing only those reports associated with the persons permissions that are established by their supervisor and in conjunction with the ISSO.

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):

System of Records Notice (SORN) State-73 GFMS.

☐ does NOT contain information covered by the Privacy Act.

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

Vendor, CS and FS employee's information is obtained from CAPPS. Employees are given notice prior to collection by CAPPS through SORN State-73 Global Financial Management System. US Citizens requesting repatriation funding are given notice through a Privacy Act Statement when completing Form DS-3072.

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

Information for repatriation funding is voluntary but the applicant may not be eligible for assistance if the information is not provided. This section is not applicable to vendor, CS and FS employees.

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. This Information is required in order to process payroll payment, advances and loans.

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.

Notice is provided to individuals at time of collection and public notice is provided in SORN State-73, Global Financial Management System. A privacy statement is available on forms associated with this collection. The notice is reasonable and adequate in relationship to the system's purpose and use.

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?

Procedures are published in the Federal Register to inform individuals how to inquire about the existence of records about them. Individuals may gain access or amend records that they believe are incorrect by submitting a request to A/GIS/IPS.

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

There are no risks associated with Notification and Redress—as it is a part of the SORN (Global Financial Management System STATE-73).

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 DARTS is limited to authorized DOS employees, and cleared contractors, who have a need for access to the system. All users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to DARTS requires a user accounted assigned by Resource Management.

Each authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of their official duties. The user access agreement includes rules of behavior describing the individual responsibility to safeguard information and prohibit activities (e.g., curiosity browsing).

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 logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

The system and database administrators are the only users with direct access to the database for the purpose of performing maintenance. All rights to information and functionality within DARTS are enforced by user profiles according to the principles of least privilege and separation of duties. All access to DARTS is logged by the operating system and/or the application, depending on the activities being performed.

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

Every user must attend a security briefing prior to receiving access to the DoS networks and getting a badge for access to DoS facilities. The briefing also includes the Privacy Act of 1974. In addition, users must complete initial and annual Cyber Security Awareness training. The training consists of computer security awareness to include the proper handling of PII.

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.

No such residual risk is anticipated. DARTS was Certified and Accredited (C&A) in February 2007. Residual risks for the application were not identified. Had residual risks been discovered during the C&A process, all risks would have to been reviewed, mitigated, and accepted by the system owner. This was not the case. The system is accredited for operation in the production environment.

11. Technologies

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

There are no Privacy risks associated with this system. All technologies in use within DARTS have been approved by the IT/CCB and are widely available to all DOS applications.

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

Not applicable

12. Security

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

DARTS ATO expires February 2010.