U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Alpha Data System (ADS**)**
Bureau/Office: Office of the Secretary (OS)
Date: October 13, 2020
Point of Contact:
Name: Danna Mingo
Title: OS Associate Privacy Officer
Email: Danna_Mingo@ios.doi.gov
Phone: 202-208-3368
Address: 1849 C Street NW, Room 7112 MIB, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of Interior (DOI) Interior Business Center (IBC) is a federal shared services provider that offers business services to many Federal agencies, including financial management services, human resources and payroll support, and information technology management. The Alpha Data System (ADS) was developed by the Payroll Systems Management Branch of IBC by using application development software and methodologies for the purpose of supporting IBC Payroll Operations Division (POD) employees who process payroll for DOI and other client Federal agencies. The ADS is comprised of multiple client-server application modules including Benefits Modules which provides functionality with historical data for retirement thrift and health benefits, Pay History and Pay Research (Audit) Modules which provides historical pay and leave data, and reissued leave and earnings statements, Debt Management Modules which contains information related to employee paycheck withholdings, Tax and Accounting Modules which provides tax functions such as W2 and 1099 statements accounting for returned checks, and Payroll Certification, and Records Management Modules that scan, index and retrieve personnel and payroll source documents. The ADS contributes directly to meeting the IBC's mission to provide quality service and innovative solutions to meet customers' business needs.

C. What is the legal authority?

Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576 and the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); 31 U.S.C. Chapter 11, the Budget and Fiscal, Budget, and Program Information; OMB Circular A-127, Policies and Standards for Financial Management Systems.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?
The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-999991241; System Security and Privacy Plan (SSP) for Alpha Data System - Payroll Applications April 19, 2019 – File name: ADS SSP 18APR19.pdf

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	**None**	No	**N/A**

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

- INTERIOR/DOI-85, Payroll, Attendance, Retirement, and Leave Records, 83 FR 34156 (July 19, 2018) which may be viewed at https://www.doi.gov/privacy/doi-notices.
- Each government agency using ADS is responsible for their own system of records notice covering the collection of data at their agency.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☐ Citizenship
☐ Gender
☒ Birth Date
☐ Group Affiliation
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☒ Financial Information
☐ Medical Information
☒ Social Security Number (SSN)
☐ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☐ Personal Email Address
☐ Mother's Maiden Name

☒ Marital Status	☒ Disability Information	☐ Home Telephone Number
☐ Biometrics	☐ Credit Card Number	☐ Child or Dependent Information
☐ Other Names Used	☐ Law Enforcement	☐ Employment Information
☐ Truncated SSN	☒ Education Information	☐ Military Status/Service
☐ Legal Status	☐ Emergency Contact	☒ Mailing/Home Address
☐ Place of Birth	☐ Driver's License	☐ Race/Ethnicity

☒ Other: *Specify the PII collected.* Work address; Age; Involuntary debt (e.g. garnishments, child support); Court orders impacting payroll; Current pay and retroactive pay adjustments; Direct deposit banking information, including bank routing and account numbers; User IDs for users of the ADS system.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒Tribal agency
☐ Local agency
☒ DOI records
☒ Third party source
☐ State agency
☒ Other: *Describe* In general, no state or local agencies are providing data for use in the system. In certain limited cases, the source of a wage garnishment could be a court judgment or a tax lien issued by a state court or a municipality. In these cases, a copy of the judgment or tax lien might be included in the system, along with information concerning the judgment.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☐ Email
☐ Face-to-Face Contact
☐ Web site
☒ Fax
☐ Telephone Interview
☒ Information Shared Between Systems
☒ Other: *Describe*

- Some personnel and payroll data is received from IBC's Federal Personnel Payroll System (FPPS). Data from FPPS is originally obtained from the client agencies.
- Certain debt-related transactions are received from the U.S. Treasury Department and third party financial services providers, including credit card companies via interface file.

- Federal employees can use the Office of Personnel Management's Employee Express, which is interfaced with FPPS, to update their own direct deposit and address information, or to obtain information on benefit accounts.

D. What is the intended use of the PII collected?

The PII collected is used to process the employee payroll of the client agencies that IBC POD serves.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

POD employees use ADS for payroll services and to provide client agencies' employees information that would assist with the POD's research and audits. Information in ADS, which are primarily from FPPS, help POD employees gather data more efficiently thereby addressing FPPS calculation issues properly.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

IBC POD provides payroll services to other bureaus of DOI.
Office of the Chief Information Officer (OCIO) customer service employees located in Denver and Reston use the following ADS modules:

IRM-LEA - Leave and Earnings Statements data is loaded into the application to allow POD staff to view and reprint statements. The data is a copy of the official information maintained in the FPPS.

IRM-PRA - Historical pay and leave data received from the FPPS is loaded into the application for view by POD staff. The data is a copy of the official information maintained by the FPPS.

PDM-DMS – Read only for Debts and collections data related to salary overpayments of active federal employees.

PSS - Payroll Operations Division Support System is used to locate information regarding specific topics. The PSS currently links information located in the Knowledge Bank, Work Instructions, Manuals and Training Materials.

YRM – Used to reprint W2s and 1099s and corrected W2s and 1099s.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Certain debt-related transactions are received from the U.S. Treasury Department.

The Federal employees can use the Office of Personnel Management's Employee Express to update direct deposit and address information, or to obtain information on benefit accounts. The data will then be transmitted from Employee Express into the FPPS system at DOI.

Information may be shared with other Federal agencies as authorized pursuant to the routine uses contained in DOI-85 system of records notice.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Data is used for payment tracking for tribal reimbursement for some BIA Educators' benefits.

☐ Contractor: *Describe the contractor and how the data will be used.*

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Certain debt-related transactions are received from third party financial services providers, including credit card companies.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Most of the data is provided from FPPS, any opportunity to decline information would be between the Federal employees and client organizations (see FPPS PIA for details). Employees don't directly have an opportunity to decline information loaded into ADS but could decline information in the client organization's consent and notice process. Client organizations and the IBC itself provide opportunity for employees to decline providing voluntary types of information that would normally be entered into ADS. Specific policies and guidance for that opportunity are defined by each client organization. An employee's ability to consent to a particular use is governed by the policies of the individual client organizations.

Client organizations may decline to send employee data to be imaged for records retention for the document imaging module of ADS. The use of ADS for document retention is voluntary.

On behalf of the clients, and for its own employees, the IBC provides statutory and regulatory reports to Office of Personnel Management, Social Security Administration, Department of Treasury, DOI credit card provider via IBC Finance and client organization including Human Resources and Finance branches/offices. Those reporting requirements are outlined in Service Level Agreements with client users of the FPPS system.

Employee consent is not needed prior to meeting those reporting requirements.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

Payroll forms filled out by individuals contain appropriate Privacy Act Statements.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the DOI-85 system of records notice.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved using employee names or social security numbers. Some data received from FPPS is referenced and retrieved using a seven digit identifier assigned to each individual in lieu of using a social security number.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

The ADS produces reports for internal use and for statutory and regulatory reports on behalf of our clients (e.g. IRS forms including W2, W2c, 1099-MISC and INT, Report of Withholdings and Contributions for Health Benefits, Group Life Insurance and Retirement, Debt Notices). These reports will be used only for purposes such as documenting tax and benefits compliance. Only authorized individuals who need the reports in order to perform their jobs will be granted access.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Client agencies are responsible for the accuracy of the data provided for use in ADS. Much of the data in ADS is obtained from other systems, such as FPPS and Employee Express. These systems contain data validation tools and editing capabilities to limit data inaccuracies. The only data in ADS provided directly by client agencies are copies of documents received from their HR offices. The copies of documents are scanned into the Document Imaging module and are used by POD employees for research.

B. How will data be checked for completeness?

Client agencies are responsible for the completeness of the data provided for use in ADS. Much of the data in ADS is obtained from other systems, such as FPPS and Employee Express. These systems contain data validation tools and editing capabilities to eliminate incomplete data entries.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

ADS contains validation tools to ensure that payroll data received for processing is for the current pay period. There are data checks built into the file loads verifying data received from FPPS and Employee Express is for current pay period and valid.

Client agencies are responsible for maintaining the currency of the data provided for use in ADS.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

The ADS applications are covered under DOI Departmental Records Schedule (DRS) and the General Records Schedule, Schedule 2; "Payrolling and Pay Administration Records". The specific disposition period depend on the subject of the record as specified in the appropriate records schedule.

DOI Departmental Records Schedule (DRS) supersedes a large number of existing GRS and non-GRS administrative records schedules. Yet there are many GRS items that remain active and in use, either due to exceptionally short retention times that can be utilized without change, or because laws or regulations prevent altering their disposition. ADS is using one of these GRS schedules – GRS 2-2 for two types of

records. For DRS 1.2B DAA-0048-2013-0001-0005 and DRS 1.3B DAA-0048-2013-0001-0011, the retention period is seven years unless there is a business need identified. In ADS some records under these schedules have a business need for 15 years.

For BIA Public Law (PBM-PLA), the DOI Departmental Records Schedule is DRS 1.2C (3) DAA-0048-2013-0001-0007. The disposition is temporary, and the Cut off starts upon separation of the employee. The records would be destroyed 60 years after cut-off.

For Credit Card Debt (PDM-CCD), the DOI Departmental Records Schedule is DRS 1.2A DAA-0048-2013-0001-0004. The disposition is temporary, and the Cut off starts at the end of the fiscal year in which final payment is made. The records would be destroyed 3 years after cut-off.

For Interface Pay System, the DOI Departmental Records Schedule is DRS 1.2A DAA-0048-2013-0001-0004. The disposition is temporary, and the Cut off starts at the end of the fiscal year in which the record is created. The records would be destroyed 3 years after cut-off.

For Treasury Offset Program, the DOI Departmental Records Schedule is DRS 1.2A DAA-0048-2013-0001-0004. The disposition is temporary and the Cut off starts when garnishment is terminated. The records would be destroyed 3 years after cut-off.

For the Retirement System Data Files, the DOI Departmental Records Schedule is DRS 1.2B DAA-0048-2013-0001-0005. The disposition is temporary, and the Cut off starts upon OPM acceptance of annual summary. The records would be destroyed 15 years after cut-off.

For Thrift Reporting, the DOI Departmental Records Schedule is (DRS 1.2B DAA-0048-2013-0001-0005). The disposition is temporary, and the Cut off starts at close of pay year. The records would be destroyed 15 years after cut-off.

For Debt Management System, the DOI Departmental Records Schedule is DRS 1.3B DAA-0048-2013-0001-0011. The disposition is temporary, and the Cut off starts at close of pay year in which debt collection is settled. The records would be destroyed 15 years after cut-off.

For W2 Corrections, DOI Departmental Records Schedule is DRS 1.2B DAA-0048-2013-0001-0005. The disposition is temporary and the Cut off starts when corrected W2 is sent. The records would be destroyed 15 years after cut-off.

For Leave and Earnings Statements, the DOI Departmental Records Schedule is DRS 1.B DAA-0048-2013-0001-0005. The disposition is temporary, and the Cut off starts at close of pay year. The records would be destroyed 15 years after cut-off.

For Collection Sub Application (PAM-CSA), the DOI Departmental Records Schedule is DRS 1.B DAA-0048-2013-0001-0005. The disposition is temporary and the Cut off starts at end of fiscal year. The records would be destroyed 7 years after cut-off.

For Electronic Certification Application (PAM-ECA), the DOI Departmental Records Schedule is DRS 1.B DAA-0048-2013-0001-0005. The disposition is temporary and the Cut off starts when final payment is made. The records would be destroyed 7 years after cut-off.

For Limited Pay Application (PAM-LPA), the DOI Departmental Records Schedule is DRS 1.B DAA-0048-2013-0001-0005. The disposition is temporary and the Cut off starts at the end of the month. The records would be destroyed 7 years after cut-off.

For Treasury Memo Application (PAM-TMA), the DOI Departmental Records Schedule is DRS 1.B DAA-0048-2013-0001-0005. The disposition is temporary and the Cut off at end of CY. Business Need Destroy 15 years after cut off.

For the Retirement and Insurance Transfer Data Files (PAM-RTA), the DOI Departmental Records Schedule is DRS 1.2B DAA-0048-2013-0001-0005. The disposition is temporary, and the Cut off starts upon OPM acceptance of annual summary. The records would be destroyed 7 years after cut-off.

For Document Imaging System (DIS) the DOI Departmental Records Schedule is DAA 048-2013-0001-0005. The disposition is temporary, and the records would be destroyed when no longer needed.

For Retirement Card Imaging (RCI) (non-record), the DOI Departmental Records Schedule is DRS 1.2A DAA-0048-2013-0001-0005. The disposition is temporary, and the records would be destroyed when no longer needed.

For Pay Audit (IRM-PRA), the record schedule is GRS 2, Item 2. The disposition is temporary and the Cut off starts when audit is finished. The records would be destroyed 15 years after cut-off.

SSA (SSA FLSA W2 & 1099) was used to generate W2 and 1099 files for transmission of data to FPPS for SSA separated employees who have received FLSA back-pay settlements. Final generation of W2 and 1099 forms for the settlement was completed in 2005.

SSA-FLSA (SSA FLSA Back Pay) is historical data in the application is used by POD staff to view historical pay and leave data. Data in the application is a copy of the official information maintained by Health and Human Services.

Records belonging to external Federal customer agencies are retained in accordance with applicable agency records retention schedules or General Records Schedules (GRS) approved by the National Archives and Records Administration (NARA), and customers are responsible for managing and disposing of their own records. Retention and disposition may vary based on the type of record and needs of the agency. The customer agency provides the IBC with the appropriate records retention schedule for the customer agency data and is responsible for managing their own records in accordance with the Federal Records Act.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Each customer agency storing data in the system maintains those records under NARA approved records schedules for the retention of reports and data. While the IBC provides system administration and management support to agency clients, any records disposal is in accordance with customer agency approved data disposal procedures and each customer agency is responsible for meeting records requirements and managing the disposition of those records at the end of the retention period.

DOI records are disposed of by shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

Customer agencies are responsible for purging employee data according to the customer agency records schedule after an employee's access authority is terminated or the employee retires, changes jobs, or dies. The IBC may purge or delete any customer payroll or personnel records if it is a requirement of the customer agency and is agreed upon in the Inter-Agency Agreement with the IBC.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There are risks to the privacy of individuals due to the volume of sensitive PII contained in the system. Potential privacy risks include lack of adequate notice, inadvertent disclosure, unauthorized access or use, collecting and retaining PII longer than necessary, and not properly disposing of records.

ADS assists in processing payroll for DOI and numerous Federal customers. The data is necessary to perform those functions and to comply with related Federal laws and regulations. The ADS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. ADS is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system. The data in ADS are mostly from FPPS which has a series of privacy controls and security controls in place. With regards to the documents sent through the mail, fax and Secure Transport, strict procedures prescribed in Client Interface Manual are being followed. The fax machine is located in POD's locked office. The documents to be scanned into the Document Imaging module are stored in the locked office. The hard copy documents are placed in a locked bin for shredding after the scan is completed. The data transmission between the secured and the unsecured networks are also protected through technical control.

Data is maintained to support agency personnel and payroll operations in accordance with approved records retention schedules. Detailed record retention schedules and disposition procedures for each different module of ADS are also documented in an official POD list.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The IBC follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training, and sign DOI Rules of Behavior.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation* The purpose of ADS is to assist in the processing of payroll and related transactions. The use of the data is both relevant and necessary for this purpose. No payments are generated within the ADS.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. The ADS does not derive new data or create previously unavailable data about individuals through aggregation from the information collected.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to data is granted on a "need-to-know" basis to authorized employees of IBC's Payroll Operations Division and OCIO Customer Support Center Staff. The Data Custodian and Security Point of Contact (SPOC) for the ADS administers access. ADS security profiles define the data that a user is permitted to access. The security point of contact (SPOC) can restrict data access based upon a user's access privilege and the "need to know". Default access is established for all positions and documented in the Front End Security Request Guide.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☐ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

☒ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*

☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system does not have the ability to identify, locate and monitor individuals. The system does contain an audit log that can be used to review the actions of users while they are accessing the system. This information includes user identification, time of access, and a list of files and data elements accessed.

M. What controls will be used to prevent unauthorized monitoring?

Access to the system is restricted to authorized personnel with valid user IDs and passwords. User accounts allow authorized personnel with valid credentials to access data. In addition, all users must complete security, privacy, and records management training before being granted access to any DOI IT resource, and annually thereafter, and sign DOI Rules of Behavior. All ADS administrative staff must also complete role based security training.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The IBC Payroll Operations Division, Chief, serves as the ADS Information System Owner and the official responsible for oversight and management of the ADS security and privacy controls and the protection of information processed and stored by the ADS system. The Information System Owner and the FPPS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in ADS.

Customer agency data in ADS is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ADS Information System Owner is responsible for oversight and management of the ADS security and privacy controls, and for ensuring to the greatest possible extent that the ADS customer agency and agency data is properly managed and that all access to customer agency and agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to the customer agency and DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures. The customer agency data in ADS is under the control of the customer agency. Each customer agency is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data.