

**PRIVACY IMPACT ASSESSMENT**  
**FRONT END PROCESSOR**

**1. Contact Information**

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

**2. System Information**

- (a) Name of system: Front End Processor
- (b) Bureau: Consular Affairs (CA)
- (c) System acronym: FEP
- (d) iMatrix Asset ID Number: 344
- (e) Reason for performing PIA: Click here to enter text.
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security reauthorization – consolidation of paperwork for legacy systems
- (f) Explanation of modification (if applicable):

**3. General Information**

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

- (b) What is the security Assessment and Authorization (A&A) status of the system?

The estimated authorization to operate (ATO) date for FEP is January 2019.

- (c) Describe the purpose of the system:

The FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications. FEP is a multi-threaded application that provides the Travel Document Issuance System (TDIS), Passport Record Imaging System Management (PRISM), American Citizen Services (ACS), Consular Lookout and Support System (CLASS), Passport Information Electronic Records System (PIERS) and Passport Lookout Tracking System (PLOTS) applications the ability to communicate with several

database systems. With one request, FEP can query multiple applications of these systems and return a consolidated response. FEP does not generate or save any new data. Its only function is to perform accurate data translation. For every data request and translation, there is a transaction record entered into the FEP database server. FEP prepares and drops batches of data for transfer to outside agencies via Consular Data Information Transfer System (CDITS). CDITS is a separate system outside of the FEP boundary.

The FEP performs the following:

- Accepts the client system request
- Places the request in the appropriate format for each database
- Sends the reformatted request
- Collects a response from each of the various databases
- Consolidates the responses
- Reformats the responses
- Sends a single consolidated reply to the requester

The FEP Automated Information System (AIS) performs the following query functions:

- Namecheck Service: TDIS, CLASS, ACS run name check verifications through FEP.
- Social Security Administration (SSA): Checks the validity of the Social Security numbers and the Death Master File; Via CDITS, FEP prepares and provides batches of SSN checks for delivery to SSA.
- Digital signature Delivery Service: TDIS uses FEP to acquire digital signatures for ePassports.
- Image Retrieval: PLOTS uses FEP for image retrieval. FEP retrieves images for requesting systems from PRISM that are sent to Department of Homeland (DHS) Security Customs and Border Protection (CBP) via CDITS.

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

The following PII elements are collected and maintained by FEP:

- Names of Individuals
- Birth dates
- Social Security Numbers
- Phone numbers of individuals
- Business Address
- Personal Address
- e-mail addresses of individuals
- Images or Biometric IDs

- Substantive family information, e.g., family assets, foreign family members, genealogical records, etc.
- Other individual information, e.g., travel history, vacations, articles, professional society memberships, etc.

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

- 5 U.S.C. 552a (Privacy Act of 1974 as amended);
- 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended (INA)), including 8 U.S.C. 1104 (Powers and Duties of the Secretary of State) and 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens); and selected non-INA sections of Title 8 as listed in the Appendix to Bender's Immigration and Nationality Act Pamphlet, 2018 edition);
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure);
- 22 U.S.C 2651(a) (Organization of Department of State);
- 22 U.S.C. 3927 (Chief of Mission);
- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and providing assistance to other agencies);
- 22 U.S.C. 211a-218, (Passports);
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number);
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);
- 22 U.S.C. 2705 (U.S. Passports and Consular Reports of Birth Abroad);
- 22 U.S.C. 2671(b)(2)(A)-(B) and (d) (Evacuation assistance and repatriation loans for destitute U.S. Citizens abroad);
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance);
- 22 U.S.C. 2151n-1 (Assistance to arrested citizens) (Repealed, but applicable to past records);
- 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts);
- 42 U.S.C. 14901-14954; Inter-country Adoption Act of 2000, as amended (Implementing legislation for the Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption, done at The Hague on May 29, 1993);
- 22 U.S.C. 9001-9011, International Child Abduction Remedies Act (implementing legislation for the Convention on the Civil Aspects of International Child Abduction, done at The Hague October 25, 1980; assistance to applicants in the location and return of children wrongfully removed or retained or for securing effective exercise of rights of access);
- 22 U.S.C. 9101, 9111-9114, 9121-9125, 9141, International Child Abduction Prevention and Return (implementing legislation for the Convention on the Civil Aspects of

International Child Abduction, done at The Hague October 25, 1980; reporting requirements, prevention measures, and other assistance on international parental child abduction cases);

- 26 U.S.C. 6039E (Information Concerning Resident Status);
- Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports);
- 22 C.F.R. Parts 50, 51 and 52 (Nationality Procedures and Passports);
- 22 C.F.R. Part 71 (Protection and Welfare of Citizens and Their Property);
- 22 C.F.R. Part 92 (Notarial and Related Services);
- 22 C.F.R. Parts 96 -99 (Intercountry Adoptions)

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

Yes, provide:

**- SORN Name and Number sand Date:**

- STATE 26, Passport Records; March 24, 2015
- STATE 05, Overseas Citizens Services Records and Other Overseas Records; September 8, 2016

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

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?  Yes  No

If yes, please notify the Privacy Division at [Privacy@state.gov](mailto:Privacy@state.gov).

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?  Yes  No

(If uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov) .)

If yes provide:

- Schedule number Department of State Records Disposition Schedule:

A-13-001-16 Passport Lookout Master

Description: This on-line information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the

issuance of full validity passport and those whose existing files must be reviewed prior to issuance.

Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)

DispAuthNo: N1-059-04-2, item 16

#### A-13-001-17 Passport Lookout Index

Description: This on-line information system provides rapid access to names in the Passport Lookout Master.

Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 27)

DispAuthNo: N1-059-04-2, item 17

#### A-13-001-18 Name Check System (NC)

Description: Name Check History Master. This series contains a yearly listing of requests by Passport Services and Visa Services personnel to query the Passport and Visa Lookout systems (see schedules for A-13-001-16 and 17). The listing provides statistical data for the Bureau of Consular Affairs.

Disposition: Destroy when active agency use ceases.

DispAuthNo: N1-059-04-2, item 18

#### A-15-001-02 American Citizens Services (ACS) system

Description: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts.

ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases; lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes biographic information, case information, and case activity log.

Disposition: TEMPORARY. Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later.

NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping.

(Supersedes NARA Job No. NI-059-96-30, Item 1 and NARA Job No. NI-084-96-4, Item 1)

DispAuthNo: N1-059-09-40, item 1

#### 4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)
- U.S. Government/Federal employees or Contractor employees
- Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

Yes  No

- If yes, under what authorization?

Executive Order 9397, November 22, 1943

Executive Order 13478, November 18, 2008.

26 U.S.C. 6039E – Information Concerning Resident Status

(c) How is the information collected?

FEP receives and transmits electronic transactions containing PII to and from Consular Affairs systems addressed in paragraph 3.c. via the State Department intranet. FEP does not originate PII or collect PII.

(d) Where is the information housed?

Department-owned equipment

FEDRAMP-certified cloud

Other Federal agency equipment or cloud

Other

- If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?

Data processed by FEP is sourced from several Consular Affairs systems. FEP is totally dependent upon the validity and accuracy of the sourcing data systems. Accuracy is the responsibility of the passport or visa applicant completing the applications for services.

External agencies providing information to the State Department are responsible for the accuracy of the information in the records that the agency submits.

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

FEP receives and transmits transactions containing PII to and from Consular Affairs systems. FEP does not update information or check if it is current. The applicant can update information by following guidance in accordance with the procedures stated in the relevant Systems of Records Notice (SORN), in addition to specific guidance provided for the system in which

services are being requested. Also, the systems that provide CA services have processes in place to ensure information is current such as face-to-face interviews and follow-ups via mail; in addition to checking information against other CA databases for discrepancies.

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

No. The FEP system does not use commercial information, and the information is not publicly available.

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

FEP does not collect personal information directly from any individuals. Information is provided from other internal databases and from external agencies prior to the electronic transfer to FEP for processing. All application forms containing PII have Privacy Act Statements stating the purposes for soliciting the information on the form. Additionally, notice of the use of personal information is provided through the two SORNs mentioned above in paragraph 3.f., STATE-05 and STATE-26.

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

- If yes, **how** do individuals grant consent?

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

FPP does not directly collect personal information from applicants; therefore, opportunity and/or right to decline options do not directly apply to this system. FEP is used to perform translation of data requests between Passport Systems' major applications.

An applicant does have the option to decline and may refuse to provide the requested information from the originating systems in which Consular Affairs services are being requested; however, doing so may result in the denial of the application.

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

The PII collected by FEP is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the

data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the systems to perform the functions for which they are intended.

## 5. Use of information

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

With one request, FEP can query multiple applications and return a consolidated response regarding crucial information in processing consular services requests such as: name check services, SSN checks, images, etc. By performing this function, the Department greatly reduces the issuance of passports to those who may pose a national security threat and/or who may be using a false identity.

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

Yes – The information collected supports the implementation of the State Department’s Consular Services programs. The information is used to support passport application submission, processing, and approval/denial decisions.

- (c) Does the system analyze the information stored in it?

Yes

No

If yes:

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

- (2) Does the analysis result in new information?

- (3) Will the new information be placed in the individual’s record?  Yes  No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?  Yes  No

## 6. Sharing of Information

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

Only authorized Department of State employees, and cleared contractors who have a justified need for the information in order to perform official duties have access to FEP data.

Internally, FEP retrieves and provides passport related images to requesting CA Systems, i.e., TDIS, PRISM, CLASS, ACS, CDITS and PLOTS.

FEP does not share any information directly with external agencies. FEP prepares and drops batches of data to Consular Data Information Transfer System (CDITS) for transfer to outside agencies: the Department of Homeland Security Customs and Border Protection (DHS/CBP) and the Social Security Administration.

(b) What information will be shared?

The data processed and shared by FEP includes PII outlined in paragraph 3.d.

The FEP Automated Information System (AIS) shares the following:

- Passport Images and Namecheck Service is shared with: TDIS, CLASS, ACS.
- Social Security Administration (SSA): Checks the validity of the Social Security numbers and the Death Master File; Via CDITS, FEP prepares and provides batches of SSN checks for delivery to SSA.
- Digital signature Delivery Service: TDIS uses FEP to acquire digital signatures for ePassports.
- Image Retrieval: PLOTS uses FEP for image retrieval. FEP retrieves images from PRISM that are sent to Department of Homeland (DHS) Security Customs and Border Protection (CBP) via CDITS.

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

The FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications within Consular Affairs. The information is used to verify applicant identities, to prevent the issuance of travel documents, passports and other requested Consular Affairs services to those who pose national security threats and/or who are using false identities or who are otherwise ineligible for a U.S. passport. The FEP system provides information to the Department's consular posts and passport agencies, the Department of Homeland Security and the Social Security Administration, for use in evaluating applicants requesting Consular Affairs services, thereby lessening the possibility of a terrorist or criminal being allowed into the United States or receiving a U.S. passport through fraud.

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

The information is shared with other Consular Affairs systems by secured internal connections via OpenNet. No information is shared externally by FEP with external organizations. CDITS shares with external organizations and is a separate system outside of the FEP boundary.

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

Information processed by FEP system is shared *internally* by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files is protected by inherited security controls from the Department of State domain infrastructure. Audit trails track and monitor usage. For every data request processed by FEP, a full record of the data transaction is entered into the FEP database server transaction logs. FEP does not transmit information *externally*.

Internal recipients within the Department of State are required to comply with U.S. government requirements for the protection and use of PII. These safeguarding requirements include, but are not limited to, security training and following internal Department policy for the handling and transmission of “Sensitive But Unclassified” information. In addition, all Department users are required to attend annual privacy and security awareness training to reinforce safe handling practices. Defense in depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring are deployed as well as role based access based on least privilege.

Supervisors along with Information System Security Officers (ISSOs) determine the access level depending on job function and level of clearance. Access to the FEP application is strictly limited to System and Database administrators. Contractor system and database administrators are the only individuals who have direct access to the system.

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

Privacy concerns regarding the sharing of information in these systems focuses on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:

Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft of information to non-authorized parties regardless whether

the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

- 1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII (sensitive but unclassified), and all higher levels of classification, and signing a user agreement.
- 2) Strict role based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level
- 3) System authorization and accreditation process along with continuous monitoring via Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

## 7. Redress and Notification

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

FEP only processes transactions containing PII that is collected by other Consular Affairs systems. The individual would need to follow processes outlined by the source system where services are requested to request access to their information. Also, the associated SORNs listed in paragraph 4.h. provide information on how to gain access to information.

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

Yes  No

If yes, explain the procedures.

FEP only processes transactions containing PII that is collected by other CA systems. The systems sourcing the data to FEP provide guidance on how to correct inaccurate information.

Additionally, procedures for individuals to correct inaccurate or erroneous information are available to the public and published in the SORNs STATE-05 and STATE-26 and in rules published at 22 CFR 171 Subpart D, Privacy Act Provisions informing individuals how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record.

If no, explain why not.

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

The FEP does not collect PII from individuals and only pulls PII from other Consular Affairs systems. Notification about procedures to correct information is provided by the source system through which the applicant is requesting services. Information is also provided in the associated SORN of the source system.

## 8. Security Controls

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

Access to the FEP is restricted to cleared, authorized Department of State FEP System and Database Administrators. The system is secured within the Department of State intranet in accordance with applicable National Institute of Standards and Technology (NIST) 800-53 and the State Department Security Configuration Guides, where risk factors are mitigated through the use of defense in-depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

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

FEP system users are limited to its System and Database Administrators. To access FEP, persons must be authorized users of the Department of State's unclassified network, which requires a background investigation and an application approved by the person's supervisor and Information System Security Officer (ISSO). Each authorized user must electronically sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. ISSOs determine the access level needed by a user to ensure it correlates to the user's particular job function and level of clearance.

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

The level of access granted to FEP restricts the data that may be viewed and the degree to which data may be modified. Administrative activity is monitored, logged, and audited.

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides, and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems (including FEP) that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with State Department Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating System (OS) Level auditing is set in accordance with the State Department Security Configuration Guides. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application logs record events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

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

In accordance with Department of State computer security policies, mandatory security (PS800 Cyber Security Awareness) and privacy (PA459 Protecting Personally Identifiable Information) training is required for all authorized users. Each user must complete the Cyber Security Awareness Training, which has a privacy component, annually. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

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

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists, are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access or data manipulation. All access to Department of State systems requires dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize that risk, and to minimize the risk, and to minimize the risk of harm to State Department programs or the public interest through an

unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

## 9. Data Access

- (a) Who has access to data in the system?

System and Database Administrators are the only personnel who have access to the FEP information.

- (b) How is access to data in the system determined?

Access is determined based on requests which are approved by the supervisor and ISSO. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

- (c) Are procedures, controls or responsibilities regarding access to data in the system documented?

Yes No

The FEP System Security Plan documents procedures, controls and responsibilities regarding access to FEP data.

- (d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Users other than the administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

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

-Access control policies and access enforcement mechanisms control access to PII. Role-based access control is implemented to restrict access to FEP data. Additionally, all user actions are audited and reviewed in accordance with State Department policy

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges, are restrictive rights/privileges or accesses needed by users for the performance of specified tasks and are implemented. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII,

along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN), and activities while logged in can be traced to the person who performed the activity.