PRIVACY IMPACT ASSESSMENT

Integrated Security and Suitability System (IS3)

1. Contact Information

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

2. System Information

Date of completion of this PIA: August 2022
Name of system: Integrated Security and Suitability System
System acronym: IS3
Bureau: DS/SI/PSS
iMatrix Asset ID Number: 6186
Child systems (if applicable) and iMatrix Asset ID Number: N/A

(a) ☐ New system
☐ Significant modification to an existing system
☒ To update existing PIA for a triennial security reauthorization

(b) Explanation of modification (if applicable): N/A

(a) Does the system have a completed and submitted data types document in Xacta?
☒ Yes ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) ☐ Yes ☒ No

If yes, has the privacy questionnaire in Xacta been completed?
☒ Yes ☐ No

(c) Describe the purpose of the system

The Integrated Security and Suitability System (IS3) is a comprehensive system that supports all functions and activities associated with the processing of personnel security, including the investigative process, reviewing existing data, updating existing records, gathering data, and making informed decisions (both positive and adverse) on eligibility for security clearances and access to classified information based on national and
Department standards. In addition, IS3 supports the record keeping requirements, management metrics, financial linkages, and litigation support needs that the above processes require. IS3 also provides a foundation for an interconnected, inter-agency security clearance management solution.

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

IS3 collects and maintains the following types of PII on U.S. persons, non-U.S. persons, and U.S. government personnel/contractors. Individuals who are the focus of investigations are referred to as “subjects”.

Subject PII includes the following:

- Name
- Personal Phone Number
- Personal Email Address
- Personal Address
- Passport Number
- National ID (for Non-U.S.-persons)
- Date of Birth
- Place of Birth
- Citizenship
- Educational
- Financial Information
- Personnel/ Employment
- Family
- Mother's Maiden Name
- Legal
- Medical
- Former Address
- Military Service/History
- Names, Residence and Nationality of Spouses, Family, Relatives, Friends and Associates
- Full Social Security number (SSN)
- Fingerprint Records

The remainder of this PIA will only focus on the PII of U.S. persons.

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

- Executive Order 12968, as amended (Access to Classified Information);
• Executive Order 13467, as amended (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information); and

(f) Is the information searchable by a personal identifier?

☒ Yes, provide:

- SORN Name and Number: Security Records, STATE-36
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

☐ 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 Office at 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.)

If yes provide (Consolidate as much as possible):
- Schedule number (e.g., (XX-587-XX-XXX)): See below table
- Disposition Authority Number: See below table
- Length of time the information is retained in the system: See below table
- Type of information retained in the system: See below table
<table>
<thead>
<tr>
<th>Schedule Number</th>
<th>Type of Information</th>
<th>Schedule Disposition Number</th>
<th>Length of Time Retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Support Records</td>
<td>Records relating to the support of security and law enforcement programs and initiatives. Records include, but are not limited to, memoranda, memorandum of agreements (MOAs); memorandum of understandings (MOUs); correspondence; congressional request or inquiries; research; policies and procedures; activities, status, or other reports; requirements; surveys; drawings; waivers; plans; studies; and investigations covering accreditation, anti-terrorism, assessments, asset forfeiture, building construction, computer security, counterintelligence, countermeasures, cybersecurity, crisis management, contractors, courier services, debugging, demolition, defensive equipment, Government-owned and commercially leased motor vehicles, electronic security, emergencies covering U.S. citizens abroad, emanations, engineering, inspections, inventories, penetration, physical security, product certification, product evaluation, program reviews, protective detail, security incidents, shielding, special events, surveillance detection, systems development, Tempest, testing, training, travel schedules, zones of control, victim resource advocacy, employee work schedules and assignments, Law Enforcement Availability Pay (LEAP) and other law enforcement personnel related matters, and other related subjects.</td>
<td>DAA-0059-2018-0003-0006</td>
<td>NOTE: NARA will be notified and an independent appraisal of Historical or Top Echelon case files that warrant permanent preservation will be conducted. Temporary. Cut-off at end of calendar year of final action. Destroy/delete 3 years after cut-off but no later than 10 years if required for business use.</td>
</tr>
</tbody>
</table>

IS3 is the Personnel Security and Suitability processing system and archive. It allows users to conduct background investigations and maintain clearances or public trust certifications on employment candidates, employees, and others seeking access to the Department of State to assure that granting an individual access to classified information is clearly consistent with the interest of national security. Data captured includes security and suitability case files with their associated standard security forms, reports of investigation, adjudicative analyses, memoranda, worksheets, authorizations, as well as out of cycle reporting information, such as foreign travel, foreign contacts, and workplace incidents. IS3 tracks the various processing steps and activities involved with investigations and the determinations made regarding security clearances, public trust certifications and suitability. The system covers the entire process and interfaces with other external databases for information.

IS3 includes Other Agency Investigation Files, Contractor Security Files, Visitor Security Files, the Department Applicant Files, and Department Employee Files.
<table>
<thead>
<tr>
<th>Schedule Number</th>
<th>Type of Information</th>
<th>Schedule Disposition Number</th>
<th>Length of Time Retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology Development Project Records—Special Purpose Computer Programs and Applications</td>
<td><strong>Special Purpose Computer Programs and Applications:</strong> Computer software programs or applications that are developed by the agency or under its direction solely to use or maintain a master file or database authorized for disposal in a GRS item or a NARA-approved records schedule. IS3 includes Other Agency Investigation Files, Contractor Security Files, Visitor Security Files, Department Applicant Files, and Department Employee Files.</td>
<td>GRS 3.1, item 012</td>
<td>Temporary. Delete when related master file or database has been deleted, but longer retention is authorized if required for business use. NOTE: NARA will be notified and an independent appraisal of Historical or Top Echelon case files that warrant permanent preservation will be conducted.</td>
</tr>
<tr>
<td>High Profile Case Files</td>
<td>Case files: Records relating to personnel security and suitability of top Echelon officials; reflecting distinctive department activities or attract media or congressional interest; concerning terrorist, criminal and other specific threats or actions taken against diplomats, American citizens, Department personnel, families, facilities or property; or documenting programs that prevent, disrupt and resolve acts of international terrorism.</td>
<td>DAA-0059-2018-0003-0002</td>
<td>Permanent. Cut-off at end of calendar year of case closure. Transfer to the National Archives 25 years after cut-off. Notify NARA for an independent appraisal. Retire 5 years after separation or closure of file. Transfer to National Archives when 25 years old.</td>
</tr>
<tr>
<td>Intermediary Records:</td>
<td>Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record. To qualify as an intermediary record, the record must also not be required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Records include: • non-substantive working files: collected and created materials not coordinated or disseminated outside the unit of origin that do not contain information documenting significant policy development, action, or decision making. These working papers do not result directly in a final product or an approved finished report. Included are such materials as rough notes and calculations and preliminary drafts produced solely for proof reading or internal discussion, reference, or consultation, and associated transmittals, notes, reference, and background materials. • audio and video recordings of meetings that have been fully transcribed or that were created explicitly for the purpose of creating detailed meeting minutes (once the minutes are created) • dictation recordings • input or source records, which agencies create in the routine process of creating, maintaining, updating, or using electronic information systems and which have no value beyond the input or output</td>
<td>GRS 5.2, Item 020</td>
<td>TEMPORARY. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. An agency must submit a notification to NARA per 36 CFR 1225.24(a)(1) prior to destroying hardcopy input records previously scheduled as permanent. An agency must schedule the electronic version of unscheduled hardcopy input records prior to destroying the input record. Legal citations: 36 CFR 1225.22 (h)(2); 36 CFR 1225.24 (a)(1)</td>
</tr>
<tr>
<td>Schedule Number</td>
<td>Type of Information</td>
<td>Schedule Disposition Number</td>
<td>Length of Time Retained</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>-----------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>transaction: hardcopy input source documents where all information on the document is incorporated in an electronic system (See Exclusion 1 and Note 1); electronic input source records such as transaction files or intermediate input/output files • ad hoc reports, including queries on electronic systems, whether used for one-time reference or to create a subsequent report • data files output from electronic systems, created for the purpose of information sharing or reference (see Exclusion 2)</td>
<td>GRS 3.2, item 050 and GRS 3.2, item 051</td>
<td>TEMPORARY. Delete/destroy incremental backup tapes when second and subsequent backup is verified as successful or when no longer needed.</td>
</tr>
<tr>
<td></td>
<td>System Backups: System backups and Tape Library Records. Backup tapes maintained for potential system restoration in the event of system failure or other unintentional loss of data.</td>
<td>SCHEDULE</td>
<td></td>
</tr>
<tr>
<td>Backups of Master Files and Databases</td>
<td>Backups of Master Files and Databases: Electronic copy, considered by the agency to be a Federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased. A. File identical to permanent records scheduled for transfer to the National Archives.</td>
<td>DAA-GRS-2013-0005-0007 (GRS 3.2, item 050)</td>
<td>Temporary. Destroy immediately after the identical records have been captured in a subsequent backup file or at any time after the transfer request has been signed by the National Archives, but longer retention is authorized if required for business use.</td>
</tr>
<tr>
<td>Backups of Master Files and Databases</td>
<td>Electronic copy, considered by the agency to be a Federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased. b. File identical to temporary records authorized for destruction by a NARA-approved records schedule.</td>
<td>DAA-GRS-2013-0006-0008 (GRS 3.2, item 051)</td>
<td>Temporary. Destroy immediately after the identical records have been deleted or replaced by a subsequent backup file, but longer retention is authorized if required for business use.</td>
</tr>
<tr>
<td>All Documentation for Temporary Electronic Records and Documentation not Necessary for Preservation of Permanent Records</td>
<td>System Documentation: Data administration records and documentation relating to electronic records that are scheduled as temporary in the GRS or in a NARA-approved agency schedule or any types of data administration records not listed as permanent in A-03-016-08a, including data/database dictionary records, data systems specifications, file specifications, code books, record layouts, metadata, user guides, and output specifications. And also the following records for all electronic records whether scheduled as temporary or permanent: software operating manuals, data standards, table and dependency descriptions, taxonomies, schemas, registries, source code, physical data model, and logical data model.</td>
<td>DAA-GRS-2013-0005-0003 (GRS 3.1, item 051)</td>
<td>Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.</td>
</tr>
</tbody>
</table>
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
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒ Yes ☐ No ☐ N/A

- If yes, under what authorization?
  • Executive Order 12968, as amended (Access to Classified Information); and
  • Executive Order 13467, as amended (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information).

(d) How is the PII collected?

- PII is collected in IS3 through manual input and automated processes. IS3 users enter PII of subjects into the system to facilitate background investigations and maintain clearances or fitness determinations on employment candidates and employees. IS3 subjects are: Current employees, Prospective employees, and Contractors seeking a security clearance, a renewal of a security clearance, or a position within the Department that requires an investigation before appointment.

Manual Input

• Subjects complete and submit standard forms (i.e. SF-86, SF-85P+PS, SF-85) via e-QIPs, and users manually enter subjects’ personal information and names of their spouse, immediate family members, and other background investigation data directly within the system.
• IS3 users manually upload the following background investigation documents that may contain PII, if applicable.
- DS-7601 Authorization to Conduct Criminal History Inquiry for Spouse or Cohabitant. (Signed by Spouse or cohabitant).
- DS-4002 Fair Credit Reporting Act (Signed by Subject).
- Additional releases may be required for specific sources or institutions, states, or countries.

**Automated**
- Automated Inputs: IS3 will maintain secure connections to both Government and commercial databases and conduct automated, record checks as needed to support investigations, and also collect PII via e-QIPs (i.e. SF-86, SF-85P+PS, SF-85).

(e) 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.

IS3 is housed in the AWS GovCloud, and a subset of data is on Department-owned equipment. The information is found in both the AWS GovCloud (a FedRAMP-certified cloud) and on Department-owned equipment located in the DOS Enterprise Server Operations Center (ESOC).

(f) What process is used to determine if the PII is accurate?

Accuracy of the information on the forms (i.e. SF-86, SF-85P+PS, SF-85) is the responsibility of the subject being investigated. They must review and verify their information prior to submission. Some of the PII in those forms is manually entered into IS3 and other PII is automatically ingested by the system. IS3 users are responsible for the accuracy of the information they enter into IS3.

IS3 Form Submission:
The forms listed below require a physical (inked) signature. Forms are printed, signed, scanned, and uploaded into IS3.
- DS-7601 Authorization to Conduct Criminal History Inquiry for Spouse or Cohabitant,
- DS-4002 Fair Credit Reporting Act any agency
- Additional releases may be required for specific sources or institutions, states, or countries.

Federal databases, subject interviews, telephonic communication, and email correspondences are used to verify PII during the background investigation process. If a
discrepancy is identified, it is documented and IS3 is updated to reflect the most current and accurate information.

In addition, the Bureau of Diplomatic Security, Office of Personnel Security and Suitability (DS/SI/PSS) Quality Assurance team performs quality surveillance and inspections to verify the quality and accuracy of investigations, to include submitted PII.

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

Subjects who are being investigated are responsible for providing current information, including PII, when their background investigation is initiated. IS3 maintains current PII for all submissions automated and manual via the latest data submitted on the subject’s security form (i.e., SF-86, SF85P+PS, SF85). Security forms and additional documents attached in e-QIP are ingested into IS3 every hour via an automated sync.

In addition, whenever a subject or individual is contacted regarding a pending investigation, the PII initially submitted must be verified for accuracy and currency. All changes (if any) are documented and updated to reflect the most current and accurate information.

This process applies for all IS3 collection processes manual input and automated described above in 3d.

(h) **Does the system use information from commercial sources? Is the information publicly available?**

IS3 uses limited commercial data. IS3 does not use publicly available information.

(i) **How was the minimization of PII in the system considered?**

During the requirements analysis phase of the system design, it was determined that full social security numbers are required and cannot be truncated. Also, IS3 is required to use a name, personal and business e-mail address, passport number, and National ID (for non-U.S.-persons). The PII collected is directly relevant and necessary to accomplish DS/SI/PSS’ mission.

IS3 collects a large PII dataset. Within IS3, the mitigation strategy is to only provide the information needed to complete a specific function, without adding any further PII than needed, internally or externally.

5. **Use of information**
   (a) **What is/are the intended use(s) for the PII?**

The intended uses for the PII in IS3 is to facilitate background investigations and maintain clearances or fitness determinations on subjects.
(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

The use of PII is relevant and necessary to facilitate background investigations and maintain clearances or fitness determinations on employment candidates and employees. IS3 is used to determine if granting a subject access to classified information is in the best interest of national security.

(c) Does the system analyze the PII stored in it? □ Yes ☒ No

If yes:
(1) What types of methods are used to analyze the PII?
(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

(d) If the system will use test data, will it include real PII?
□ Yes □ No ☒ N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal:
Some PII is shared with the DS Business Services Suite (DS BSS), iMatrix #104984, owned by Diplomatic Security.

External:
Limited PII listed in Question 3(d) will be shared externally with the following organizations:
- Department of Defense (DoD)
- Federal Bureau of Investigation (FBI)
- Office of the Director of National Intelligence (ODNI)

(b) What information will be shared?

Internal:

PII shared with the DS Business Services Suite:
• Full Name, Date of Birth, Full SSN, and Personal Address

External:
The following PII is shared externally:
• Department of Defense (DoD):
  o Full SSN, Last Name, First Name, Middle Name, Date of birth, and Place of Birth
• Federal Bureau of Investigation (FBI):
  o Full SSN, Last Name, First Name, Middle Name, Date of Birth, and Place of Birth
• Office of the Director of National Intelligence (ODNI):
  o Full SSN, Last Name, First Name, Middle Name, Date of Birth, Place of Birth, and Personal Address

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

Internal:
The purpose of sharing information with DS BSS is to contribute to a centralized system (web service) that is leveraged by other Department systems to verify security clearance information for employees and contractors.

External:
The purpose for sharing the information, with the external entities listed in 6(a), is to conduct Federally mandated checks of Federal databases for background investigations and to share clearance information with the required Federal agencies.

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

Internal:
DS BSS application queries on demand IS3 and retrieves the requested information.

External:
For all external sharing IS3 users generate files from IS3 and manually upload them into the external Federal databases.

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

Internal:
All communications between IS3 and DS BSS are encrypted. Only required PII (listed in 6b) is transferred between the two systems. Both systems have current anti-virus software and the most current operating system patches. All system servers are hardened using department security configuration guides.

External:
Sharing between IS3 and all external entities is safeguarded using controlled user groups both within IS3 and the external recipients of the information (FBI, ODNI, and DoD). These controlled group members receive extensive training and information on federal requirements and databases. Only the members of the controlled user groups upload documents and all communication shared with external agencies is encrypted and transmitted securely through SSL.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, notice is provided to record subjects at the point of collection via Privacy Act Statements (PAS) provided on the following forms completed for the investigation process: DS-7601 Authorization to Conduct Criminal History Inquiry for Spouse or Cohabitant and the DS-4002 Fair Credit Reporting Act.

Notice to records subjects completing e-QIPs forms is the responsibility of Office of Management and Budget (OMB) and the Federal Bureau of Investigation (FBI).

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒ Yes ☐ No

If yes, how do record subjects grant consent?

Record subjects have the opportunity to decline to provide the information requested, however, that would result in the cession of the background investigation and disqualifying them from the position for which they are applying.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

IS3 contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Individuals are entitled to avail themselves of the procedures outlined in 22 C.F.R. Part 171 in order to seek access to their own information. Individuals can submit a request to the DS Freedom of Information & Privacy Acts Division (DS/MGT/FOIA-PA). DS/SI/PSS coordinates FOIA requests with DS/MGT/FOIA-PA and processes any requests for IS3 information through that office.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?
☒ Yes  ☐ No

If yes, explain the procedures.

The procedures in 22 C.F.R. Part 171 inform the individual about how to inquire about the existence of records about themself, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act (5 U.S.C. 552a) provisions for notification and readiness may exist for certain portions of passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C.3065. These exemptions are published as agency rules at 22 C.F.R. Part 171.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Procedures to correct the information is detailed in System of Records notice titled Security Records, STATE-36 and 22 C.F.R. Part 171 in order to seek redress of their own information.

If a subject’s PII changes (e.g., name change) after their background investigation is completed, the employee or contactor must email DS/SI/PSS to inform them of such a change. IS3 is then updated to reflect the updated PII.

8. Security Controls

(a) How is all of the information in the system secured?

IS3 adheres to FIPS 140-2 certification using Oracle Transparent Data Encryption (TDE). The tablespaces used by the IS3 system are encrypted.

Additionally, IS3 has the appropriate management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002, and the information assurance standards published by NIST Special Publications 800-Series (NSIT SP 800-84). These controls include multifactor authentication (MFA), Encryption in Transit (EIT), and Data Encryption at Rest (DAR).

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

<table>
<thead>
<tr>
<th>Role</th>
<th>Privileges and Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS3 Users</td>
<td>Users are responsible for collecting, verifying, and processing all PII in IS3 to facilitate the background investigation and adjudication process for the</td>
</tr>
</tbody>
</table>
Department. The users can create, read, update, and search data in the system based on their role in the background investigation process and their need-to-know.

<table>
<thead>
<tr>
<th>Internal Department of State Users</th>
<th>They have restricted roles and use IS3 to verify security clearances and review personnel security actions to support their office’s mission. They have read only access to all PII and cannot create or update information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>System administrators establish system accounts, configuring access authorizations (i.e., permissions, privileges), review and audit event logs, implement configuration changes, troubleshoot and triage system issues, and build custom reports and queries to business requirements. Administrators don’t have access to PII.</td>
</tr>
</tbody>
</table>

(c) **Describe the procedures established to limit system and data access to only those individuals who have an “official” need to access the information in their work capacity.**

IS3 resides on the Department’s OpenNet and will inherit both local network and remote access controls. In addition to the network access controls, IS3 enforces a limit of three consecutive invalid access attempts by a user during a 15-minute timeframe. After 20 minutes of inactivity, a session lock control is implemented at the network layer. All users will have an IS3 account login, and access control constraints are put on the system using account types to ensure that individuals using the system cannot access more information than is needed to complete their function.

(d) **How is access to data in the system determined for each role identified above?**

IS3 users, Internal Department of State Users, and Administrators request access via the AccessDS application. Supervisor, Business Owner, and Information System Security Officer (ISSO) are included in the approval chain for all accounts.

(e) **What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?**

In addition to Department and AWS GovCloud standard security controls, IS3 is placed behind a virtual firewall to further limit access to system data. All user actions (e.g., adding or updating a record) within the system are recorded and maintained in a log for auditing. IS3’s data-at-rest is encrypted.

IS3 employs a robust event monitoring and reporting capability allowing tracking of activity to the file level and recording date, time, user and action.
(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?
☒ Yes ☐ No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All users are required to complete Cyber Security Awareness Training (PS800), which encompasses computer security and privacy awareness, and must complete refresher training annually in order to retain access. All Department employees are required to take the biennial privacy training “Protecting Personally Identifiable Information” (PA318).