Integrated Security and Suitability System (IS3)

1. Contact Information

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

2. System Information

(a) Name of system: Integrated Security and Suitability System

(b) Bureau: DS/SI/PSS

(c) System acronym: IS3

(d) iMatrix Asset ID Number: 6186

(e) Reason for performing PIA:

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

(f) Explanation of modification (if applicable):

S2MS is renamed to IS3; they will have the same iMatrix Asset ID.

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 for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The system received an Authority to Operate (ATO) on March 30, 2016. This ATO expired on March 31, 2017. Re-assessment activities were underway as of November 9, 2016, with A&A steps 1 through 4 submitted to IRM/IA. Completion of Step 5 is pending approval of this PIA. A&A estimated completion is December 15, 2018.

(c) Describe the purpose of the system:
Integrated Security and Suitability System (IS3) will be a comprehensive system that supports all of the 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, access, and suitability based on national and Department standards. In addition, IS3 will support the record keeping requirements, management metrics, financial linkages, and litigation support needs that the above processes require.

IS3 is currently under development and will replace several legacy systems, reengineer and automate current legacy and paper-based processes, and provide 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:

The information listed below will be collected and maintained for the purpose of supporting the investigation and adjudication of security clearance applications.

PII Provided by Subject

The primary source of the information collected is provided by the Department of State employee, prospective employee, or contractor seeking a security clearance, a renewal of a security clearance or a position with the Department of State that requires an investigation before appointment. (This individual is called “Subject".)

Subject PII includes:

- Name of an individual;
- Date and place of birth;
- Social security number;
- Other Names used;
- Mother's maiden name;
- Fingerprint;
- Gender;
- Height;
- Weight;
- Hair color;
- Address;
- Telephone numbers;
- Citizenship and status;
- Passport number(s) and issuance information;
- Citizenship or naturalization information;
- Alien registration number, if applicable;
- Current and previous residences;
- Current and previous schools attended;
- Current and previous employers.

References Provided by Subject and Verifications

Additionally, references, to include PII of other individuals, are provided by the subject. These references allow investigators to verify the accuracy of the information provided by the subject, and evaluate individual backgrounds in accordance with the "whole person concept" described in ICPG 704.1, the Federal Adjudicative Guidelines and 5 CFR 731.

References include:

- Names, addresses, phone number, social security number, date of birth, place of birth, country of citizenship, and document number for immediate family members;
- Names, addresses and phone numbers of references for each residence, school, and employment;
- Names, addresses and phone numbers of personal references;
- Name, country of citizenship, country of residence for close personal foreign Contacts;
- Names and addresses of foreign citizens sponsored to come to the U.S.;
- Names and addresses of certain medical providers;
- Names of creditors for all financial obligations;
- Names of other parties involved in any public record civil court actions.

Each of these references may be contacted to verify relevant subject information. The results of these verifications are stored in IS3.

National Agency Check for Subject and Spouse

Spousal and cohabitant information may be collected as part of their spouse or cohabitant's investigation. The Department may conduct a National Agency Check (NAC) or in limited cases Single Scope Background Investigations (SSBI), without fingerprint cards, on an investigated subject's spouse or cohabitants. In limited circumstances, a background investigation may be performed on a spouse who is a foreign national; in those cases, the same privacy controls described in this Privacy Impact Assessment would apply to the spouse's investigation. By definition, a NAC requires the indices of the following U.S. Government organizations to be queried:

(a) DoD's Defense Clearance and Investigations Index (DCII);
(b) DoD's Joint Personnel Adjudication System (JPAS);
(c) DNI's Scattered Castles Database;
(d) Investigative and criminal history files of the FBI;

(e) OPM's Security/Suitability Investigations Index (SII);
(f) Depending on the subject's background, other U.S. Government, commercial, or private organizations, and databases will be queried.

The indices of the following organizations must also be queried for a NAC, as applicable to the individual's background, to verify relevant immigration records:

(a) Department of Homeland Security;
(b) Department of State; and
(c) Director of National Intelligence

The results of the NACs for both subjects and spouses, as applicable, will be stored in IS3.

Local Agency Checks

Subject checks will also include criminal history records checks in applicable local law enforcement agencies.

Cross Reference Indices

Individual records in IS3 will store an identifier for a corresponding individual record, if one exists, in the following systems: ACES (DoD), DCII (DoD), PIPS (OPM), JPAS (DoD), CVS (OPM), eQIP (OPM).

Credit Checks

Tri Credit Bureau information will be obtained through an electronic interface. There will be a secure two-way transmission for the request of a credit check on the subject and the return of the results of a consolidated, merged credit history report.

IS3 User Account Information

IS3 will also contain PII of Department of State employees and contractors who will be users of the system, including Human Resources personnel, PSS Background Investigation Coordinators (BICs), Investigators, Quality Assurance personnel, PSS Managers, Accounting staff, and Hiring Managers.

IS3 User PII includes:

- Name;
- State Global Identifier (SGID) (login);
- Work Address;
- Phone Numbers;
- Email Address.

Invoicing and Payment Information

IS3 will provide support for investigator invoicing and payments. Investigator PII may also include:

- Tax ID;
- Contract Number;
- Mailing Address;
- Banking Routing Number.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to IS3, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended);
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and
- Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism);
- Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans);
- Executive Order 12968. 8/2/95 (Access to Classified Information);
- Executive Order 10450, 4/27/53 (Security Requirements for Government Employment); and
- Intelligence Community Policy Guidance 704.1

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

☒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): December 15, 2015

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

(f) 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.

(g) 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:
- Schedule number (e.g., (XX-587-XX-XXX)):
- Length of time the information is retained in the system:
- Type of information retained in the system:

1. Integrated Security and Suitability System **(**IS3**) (previously named "S2MS" and will replace DoS Clearance)**

Description: 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, DOS Applicant Files, and DOS Employee Files.

See individual items related to Master Case Files

Disposition: N/A

DispAuthNo: N/A

2. Integrated Security and Suitability System **(**IS3**) (previously named "S2MS" and will replace DoS Clearance)**

Description: Master case files

An electronic tracking system used to control and document background investigations and maintains 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 includes: Other Agency Investigation Files, Contractor Security Files, Visitor Security Files, DOS Applicant Files, and DOS Employee Files.

Disposition: Temporary. Destroy/delete master file data 20 years after separation of employee.

NOTE: NARA will be notified and an independent appraisal of Historical or Top Echelon case files that warrant permanent preservation will be conducted.

DispAuthNo: N1-059-08-18, item 1a(8)

---

3. Integrated Security and Suitability System (IS3**)**

Description: Employee Files
(1) Top Echelon Files, including Secretaries of State and VIPs

Note: Recordkeeping copy limited to paper.

Disposition: Permanent. Retire 5 years after separation or closure of file. Transfer to National Archives when 25 years old.

DispAuthNo: N1-059-08-18-item 1a(6)

---

4. Integrated Security and Suitability System **(**IS3**)**

Description: Employee Files

(2) Historical Files. Cases that reflect distinctive Department activities, attract media or Congressional interest, or are otherwise historically significant

Note: Recordkeeping copy limited to paper.

Disposition: Permanent. Designate as permanent at the time case takes on significance. Notify NARA for an independent appraisal. Retire 5 years after separation or closure of file. Transfer to National Archives when 25 years old.

DispAuthNo: N1-059-08-18-item 1a(7)

---

5. Integrated Security and Suitability System **(**IS3**)**

Description: Transitory and Intermediary Records

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 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)

Exclusion 1: This item does not allow destruction of original hardcopy still pictures, graphic materials or posters, aerial film, maps, plans, charts, sound recordings, motion picture film, or video recordings once they are digitized. Agencies must follow agency-specific schedules for these records. If the records are unscheduled, the agency must submit a schedule for them.
Exclusion 2: This item does not include the following data output files (agencies must follow agency-specific schedules for these records, except for the final bullet, which the GRS covers in another schedule): • files created only for public access purposes • summarized information from unscheduled electronic records or inaccessible permanent records • data extracts produced by a process that results in the content of the file being significantly different from the source records. In other words, the process effectively creates a new database file significantly different from the original • data extracts containing Personally Identifiable Information (PII). Such records require additional tracking and fall under GRS 4.2, item 130 (DAA-GRS-2013-0007-0012)

Note 1: 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)

Disposition: TEMPORARY. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

DispAuthNo: GRS 5.2, item 020

---

6. Integrated Security and Suitability System **(**IS3**)**

Description: 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.

Disposition: TEMPORARY. Delete/destroy incremental backup tapes when second and subsequent backup is verified as successful or when no longer needed.

DispAuthNo: GRS 5.2, item 020

---

7. Integrated Security and Suitability System **(**IS3**)**

Description: System Documentation

Includes systems requirements, system design, and user guides.

Disposition: TEMPORARY. Destroy or delete when superseded or obsolete, or upon authorized deletion of the related master file or data base, or upon the destruction of the output of the system if the output is needed to protect legal rights, whichever is latest.

DispAuthNo: GRS 5.2, item 020

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

☒Yes ☐No

- If yes, under what authorization?
  - Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended);
  - Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT ACT); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
  - Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

(c) How is the information collected?
PII will be collected in IS3 through both manual input and automated processes.

Manual Input

- Applicant Portal: Subjects will enter their personal information and names of their spouse, immediate family members, and references directly through this external system.
- Field Investigators Portal: Investigators will enter in results of database checks, third party application checks, and investigation reports.

Automated

- Automated Record Checks: IS3 will maintain secure connections to both Government and commercial database and conduct automated record checks as needed to support investigations

Several forms, listed below, will require physically signed forms and will be printed, signed, scanned and uploaded into IS3:

- 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)

- Form 86-1 Authorization of Release of Medical Information (Signed by Subject)
- Additional releases may be required for specific sources or institutions, states, or countries.

(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?
The individual being investigated will be responsible for submitting true and accurate information. IS3 will require subjects to review and verify their information prior to submission, and incomplete submissions will not be accepted by the system.

In addition, any agency or external source providing the information will be responsible for verifying accuracy. Specific methodologies for verification employed by Diplomatic Security (DS) will include, among other things, maintaining the system as a live feed, allowing the information to be updated/edited at any time, and cross referencing information with the DS/SI/PSS analyst or surrogates. Information found to be in error will be verified and updated by designated DS/SI/PSS Administrators.

Completeness of data will be checked through investigations and/or through personal interviews with the subject and sources holding the information.

A DS/SI/PSS Quality Assurance manager performs quality surveillance and inspections on operational processes to verify the accuracy of investigations. A case manager reviews and approves Reports of Investigation (ROIs).

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
IS3 is currently in a non-production "pilot" mode and data can be deleted periodically. Once IS3 is fully in production, only authorized users can access the IS3application. The system will have current information based on the most recently submitted eQIP/SF-86 data, which is ingested on an ongoing basis as needed to support new background investigations. An IS3service runs every few minutes to ingest XML and attachments into the IS3system. Once the file(s) are ingested, the files are deleted from the network shared folder and subdirectory and saved into a secure database.

(g) Does the system use information from commercial sources? Is the information publicly available?
IS3 will use the following types of commercial information:

- Lexis-Nexis will be used to provide data sources to provide Tri-Credit Bureau credit reports. This information will be obtained through an electronic interface that supports a secure two-way transmission mechanism for the request of a credit check on the subject and the return of the results of a consolidated, merged credit history report. This credit report information will be used to make an adjudicative decision based on 13 adjudicative guidelines outlined in Executive Order 12968 and ICD 704. This is a current business process that will not change from existing processes.
- IS3 will use Local Agency data sources that provide information from local law enforcement agency (e.g., sheriff's office, county police, and college police for a given location) investigations.

IS3 will use the following types of Government information:

- Department of Defense (DoD) databases (JPAS and DCII) will be used to provide information about prior or current clearances held and prior or ongoing investigations. This information will be obtained through electronic interfaces that support a secure two-way transmission mechanism for the request of clearance and investigation information. This information is used to determine what type of background investigation is required and if reciprocity can be granted.
- Federal Bureau of Investigations (FBI) databases of investigative and criminal history files will be used to provide information on a candidate's prior criminal history. This information is currently obtained through a dedicated secure data circuit, and will continue to be obtained through the same method to support IS3. This information is used as part of the adjudicative process to determine the suitability of the subject undergoing the investigation to obtain or maintain a position of trust or clearance.
- Office of Personnel Management (OPM) databases of previously conducted investigations, clearances, and adjudications: Suitability Investigations Index (SII) and Clearance Verification System (CVS).

(h) Is notice provided to the individual prior to the collection of his or her information?
Notice of the purpose, use and authority for collection of the submitted information are detailed in the System of Records notice titled STATE-36 and are provided via two Privacy Act Statements (one from OMB and one from the FBI).

(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?
The individual is provided copies of the Privacy Act Statement, whereby, the acknowledgement of the Privacy Act Statement signifies the individual’s consent to the use of his or her information.

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

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Several specific privacy risks related to IS3 were identified early on and controls were put in place to mitigate these risks.

Additionally, IS3 will have all 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 will include regular security assessments, physical and environmental protection, encryption, access control, personnel security, security and privacy awareness training, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports.

5. Use of information

(a) What is/are the intended use(s) for the information?
The information is used to support the background investigation process. It allows the government to make a determination on the suitability of the subject to obtain a security clearance to access certain Department information and physical locations.

(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. All elements of PII data collected and stored in IS3 are used to support the background investigation process.

(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?
IS3 will automatically analyze and generate recommended investigation plans based on the criteria and rules engine, including auto-scoping of leads and assignment of investigators.

(2) Does the analysis result in new information?
The analysis results in recommended investigation plans, including auto-scoping of leads and assignment of investigators.

(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.
Internal: IS3 will be utilized by all organizations within DS that conduct background investigations for DS/SI/PSS (i.e. Regional Security Offices, Assistant Regional Security Officers and Field Investigators).

External: IS3 will be shared with the Office of Personnel Management (OPM) through the Clearance Verification System (CVS) and Personnel Investigations Processing System (PIPS). In addition, information is shared with the Office of the Director of National Intelligence (ODNI) through Scattered Castles (SC).

(b) What information will be shared?
The information may include names, dates, places of birth (POB), Social Security Numbers (SSN), height, weight, hair color, and eye color.

(c) What is the purpose for sharing the information?
Only enough information will be shared for the investigator to ensure that all the leads are scoped and conducted to fulfill the Investigation Guidelines. Additionally, only enough information will be shared to allow other government agencies to validate the clearance of DOS employees.

(d) The information to be shared is transmitted or disclosed by what methods?
Information will be sent via leads to a specified individual within IS3. 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.

(e) What safeguards are in place for each internal or external sharing arrangement?
Internal: Selected information collected and maintained by IS3 will be shared throughout the Department through limited access controls. Numerous management, operational and technical controls will be put in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege and personnel screening. IS3 has logical access controls, and access is permission based. Only users working on a specific subject/case, will get access to that information, and only while assigned to it.

External: Tri-Credit Bureau credit information will be obtained through an electronic interface that supports a secure two-way transmission mechanism for the request or credit check on the subject. The returned result consists of a consolidated, merged credit history report. The security requirements for this transmission will meet Federal Information Processing Standard (FIPS) 140-2. The Department will utilize a VPN connection with

FTP. The requested and returned reports will be in the Extensible Mark-up language (XML), MIISMO 2.3 format.

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

IS3 will be collecting a large dataset with PII. Within IS3, the mitigation is to only provide the information needed to complete a specific lead within the application, without adding any further PII than needed, internally or externally. When sharing subject related information, consideration is given to minimize the amount of data being shared, by updating the SOPs behind the processes, and implement these changes into the IS3 application.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
IS3 contains Privacy Act-covered records; therefore, notification and readiness 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 FOIA office. PSS coordinates FOIA requests with DS/MGT/FOIA-PA, and processes any requests for IS3 information through that office.

(b) Are procedures in place to allow an individual 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 them, 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 a 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.

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

Notice of the purpose, use and authority for collection of the submitted information are detailed in the System of Records notice titled STATE-36. Individuals are entitled to avail themselves of the procedures outlined in 22 C.F.R. Part 171 in order to seek redress of their own information.

8. Security Controls

(a) How is the information in the system secured?
IS3 adheres to FIPS 140-2 certification through the use of Oracle Transparent Data Encryption (TDE). The tablespaces used by the IS3 application are encrypted.

(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.
IS3 will reside on DOS's OpenNet and will inherit both local network and remote access controls. In addition to the network access controls, IS3 will enforce a limit of three (3) 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.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Diplomatic Security (DS) uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the IS3 components, for changes to the DoS mandated security controls. In addition to the department level standard security controls, IS3 will employ a robust event monitoring and reporting capability allowing tracking of activity to the file level and recording date, time, user and action.

(d) Explain the privacy training provided to authorized users of the system.
All users will be required to undergo Cyber Security Training, which encompasses computer security and privacy awareness, prior to accessing the system, and must complete refresher training yearly in order to retain access. Federal employees are required to take Privacy training in the form of PA- 459, Protecting Personally Identifiable Information (PII). In addition, users will be required to sign a user agreement stating that they understand they are not allowed to use IS3 and the information contained within for any purpose that may be other than official.

(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.
Several steps will be taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system generates audit trails which can be analyzed and reviewed in the event that misuse of the system is suspected. An audit trail provides a record of which

particular functions a particular user performed, or attempted to perform, on an information system.

(f) How were the security measures above influenced by the type of information collected?
These security measures were implemented as a direct result of the system collecting Personally Identifiable Information (PII) and were determined to be sufficient to protect this type of information.

9. Data Access

(a) Who has access to data in the system?
Only authorized IS3 users have access to the data in the system.

(b) How is access to data in the system determined?
Access to data in the system is determined based on user role, permissions and tags associated with authorized IS3 users.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
There are different user roles with different access permissions. The level of access for a given user role will restrict the data that may be seen and the degree to which data may be modified.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
All users will undergo initial and annual refresher training and will only be granted IS3 access and role-based permissions on an as-needed basis. The system use notification ("warning banner") will be displayed before log-on is permitted, and will recap the restrictions on the use of the system. Activity by authorized users will be monitored, logged, and audited.