Privacy Impact Assessment
for the

# Select Agent Inventory

Plum Island Animal Disease Center

**DHS/S&T/PIA-031**

**December 21, 2016**


**Contact Points**
**Frank Cortese or Anne Drury**
**Plum Island Animal Disease Center**
**Science and Technology Directorate**
**(631) 323-3200**

**Reviewing Official**
**Jonathan R. Cantor**
**Acting Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

# Abstract

The Select Agent Inventory (SAI) system is a database and workflow software product used by Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Plum Island Animal Disease Center (PIADC) to house and automate requirements in support of the Federal Select Agent Program. The Federal Select Agent Program oversees the possession, use, and transfer of biological select agents and toxins that have the potential to pose a severe threat to public, animal, or plant health or to animal or plant products. The SAI database contains information on individuals who have access to PIADC and biological agents and toxins deemed "select agents". S&T is conducting this Privacy Impact Assessment because personally identifiable information (PII) is used to support SAI.

# Overview

The Federal Select Agent Program protects the nation from the accidental or intentional introduction of foreign animal diseases (FAD) that can seriously threaten livestock industries, food safety, and the economy.[1] The Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Plum Island Animal Disease Center (PIADC) houses plant and animal biological agents and toxins and automates the process of managing these agents in support of the Federal Select Agent Program. PIADC is a biosafety-level 3 laboratory and the only one in the nation that can conduct diagnostic testing, research, and vaccine development for FADs such as foot-and-mouth disease (FMD).[2] Select agent regulations require increased security for personnel and address the reliability of an individual for access to Tier 1 biological select agents and toxins (BSAT), but not for employment in general.

The Select Agent Inventory (SAI) system provides PIADC with basic database management and workflow software tools that are configured to manage resources, facilitate collaboration with colleagues, prepare reports, and coordinate end user authorizations. Personally identifiable information (PII) from end users is stored in the SAI, and that data, along with additional PII, is sent to the Federal Bureau of Investigation Criminal Justice Information

[1] The Federal Select Agent Program oversees the possession, use and transfer of biological select agents and toxins, which have the potential to pose a severe threat to public, animal or plant health or to animal or plant products. The Program develops, implements, and enforces the Select Agent Regulations; maintains a national database; inspects entities that possess, use, or transfer select agents; ensures that all individuals who work with these agents undergo a security risk assessment performed by Federal Bureau of Investigation (FBI)/Criminal Justice Information Service (CJS); provides guidance to regulated entities on achieving compliance to the regulations; and investigates any incidents in which non-compliance may have occurred.

[2] A biosafety-level 3 laboratory is one in which work is performed with indigenous or exotic agents that may cause serious or potentially lethal disease through the inhalation route of exposure.

Services Division (FBI CJIS) on the FBI Form[3] for background investigation purposes. The FBI Form is filled out and mailed to the FBI as a result of a new Select Agent Program Individual requiring access to the PIADC. The FBI Form is received by FBI CJIS and reviewed by FBI CJIS Security. FBI CJIS then returns the Bioterrorism Security Risk Assessment and newly generated FBI Unique Identification Number (UIN) to complete the background check to DHS PIADC.

The SAI, owned by DHS, contains the names and agency affiliations of personnel who have access to PIADC and identifies those personnel that have been cleared for access to select agents. Further, the SAI houses a personal identifier that has been generated as a result of the FBI CJIS process. The FBI CJIS-generated number is called the FBI UIN, and it serves as the authorization for individuals to access select agents. The FBI generates a FBI UIN each time a new individual's information is submitted for background checks. This includes background check submissions from federal, state, and local governments, as well as private companies. Additional information collected and stored in the SAI database include Date of Birth (DOB), Social Security number (SSN), system logins (username and password), each individual's access to and storage location of select agent information, as well as biological samples.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science & Technology Directorate (S&T) to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support Research & Development related to improving the security of the homeland.

The Department's authority for this collection for the purpose of security of DHS property facilities is primarily 5 U.S.C. § 301 on Government Organizations and Employees; the Homeland Security Act of 2002; Executive Order (E.O.) 9397 as amended by E.O. 13478; E.O. 12968; and Title 41, Subtitle C, Chapter 101 Federal Property Management Regulations, issued July 2002.

[3] *See* FBI CJIS FD-961, Bioterrorism Security Risk Assessment Form *available at* https://www.fbi.gov/file-repository/fd-961-for-internet.pdf/view.

9 CFR § 121 implements the provisions of the Agricultural Bioterrorism Protection Act of 2002 setting forth the requirements for possession, use, and transfer of select agents and toxins.[4] The biological agents and toxins listed in this part have the potential to pose a severe threat to public health and safety, to animal health, or to animal products. Overlap select agents and toxins are subject to regulation by both the Animal and Plant Health Inspection Service (APHIS) and Centers for Disease Control and Prevention (CDC).

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act Of 2001 (USA PATRIOT Act), Section 817, prohibits restricted persons from possessing, shipping, or transporting select agents, biological agents, and toxins.[5]

## 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following Privacy Act System of Records Notices apply to the collection, use, maintenance, and dissemination of SAI information:

- DHS/ALL-023 Department of Homeland Security Personnel Security Management,[6] covers processing records of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position; and
- DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management,[7] covers collection and maintenance of records associated with DHS facility and perimeter access control, including access to DHS information technology and access to classified facilities, as well as visitor security and management.
- JUSTICE/FBI-009 The Next Generation Identification (NGI) System[8], covers the collection and maintenance of identification and criminal history records collected during background checks for persons who provide biographic and biometric data for the purposes of security clearances and suitability determinations.

[4] Title II, Subtitle B of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188.
[5] USA PATRIOT ACT of 2001, Pub. L. No. 107-56.
[6] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010) *available at* www.dhs.gov/privacy.
[7] DHS/ALL-024 Department of Homeland Security Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010) *available at* www.dhs.gov/privacy.
[8] JUSTICE/FBI-009 The Next Generation Identification (NGI) System, 81 FR 27283 (April 26, 2016) *available at* https://www.federalregister.gov/documents/2016/05/05/2016-10120/privacy-act-of-1974-systems-of-records.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

The SAI system has a Security Plan (SP) in place which is maintained in DHS Information Assurance Compliance System (IACS). The SAI SP details the managerial, operational, and technical controls that are in place to protect the system and the data contained within it. The SP will be in place for three years and then undergo a review. The SP also explains all preventative controls including physical security and technical safeguards, such as password protections and access controls, which are consistent with the information security and physical security requirements per DHS policy.

### 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. With regard to retention schedules and file plans for "Biological Select Agent and Toxins Records," these are currently unscheduled and with NARA for determination. DHS proposes to delete the records after 6 years. Until NARA approves the final retention schedule, the records are deemed permanent and cannot be destroyed. DHS deletes user access request information after 6 years pursuant to General Records Schedule 3.2 item 031.

### 1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Federal Bureau of Investigation Bioterrorism Preparedness Act: Entity/Individual Information form FD-961, OMB No. 1110-0039, is used to capture information for FBI CJIS to determine if PIADC personnel are approved to access select agents. PIADC does not keep any copies of this form. The original is forwarded to the FBI.

One of the fundamental elements of the select agent regulations is to keep select agents and toxins out of the possession of individuals who might intend to misuse them. The Federal Select Agent Program works closely with FBI CJIS to identify those individuals who are prohibited from access to select agents and toxins based on the restrictions identified in the USA PATRIOT Act. CJIS conducts security risk assessments of all individuals, Responsible Officials (RO), Alternate Responsible Officials (ARO), and non-governmental entities that request access to select agents and toxins. The Federal Select Agent Program authorizes access to select agents and toxins based on the results of the security risk assessment.

Federal Select Agent Program (FSAP) APHIS/CDC Form 1, Application for Registration for Possession, Use, and Transfer of Select Agents and Toxins Section 4A, 4B and 4C, OMB NO. 0579-0213 and OMB NO. 0920-0576, is used to capture information for the Federal Select

Agent Program Office to assign an FBI Unique Identifying Number (or Department of Justice - DOJ Number) for the applicant's application.[9] A hard copy of this form is kept by the PIADC RO/ARO in a locked office. The retention period for this documentation is pending NARA's determination in 1.4 above.

FBI CJIS FD-961, Bioterrorism Security Risk Assessment Form, is used to capture information used by the FBI when accomplishing a background check at DHS PIADC's request.

PlADC General User Request Form, IT-007-1, is used to capture information necessary for the Information Technology Office to ensure that personnel requesting access to SAI have been fully vetted prior to access. That access is limited to information approved by their respective supervisor, and required to support their duties. None of the information collected on the IT-007-1 is entered into SAI. A hard copy of the form is held by the IT department in the access-controlled Server Room. The retention period for this documentation is pending NARA's determination in 1.4 above.

# Section 2.0 Characterization of the Information

## 2.1 Identify the information the project collects, uses, disseminates, or maintains.

The SAI system captures the following PII:

- Name;
- Date of Birth;
- SSN;
- Agency;
- Position;
- User Name; and
- Password.

Information captured on the Federal Select Agent Program Form 1 may include:

[9] 4A is for laboratorians and Animal Care Staff: http://www.selectagents.gov/resources/APHIS-CDC_Form_1_Section_4A.pdf; 4B is for Support Staff: http://www.selectagents.gov/resources/APHIS-CDC_Form_1_Section_4B.pdf; 4C is for unescorted visitors: http://www.selectagents.gov/resources/APHIS-CDC_Form_1_Section_4C.pdf; 1A is for Responsible Official, Alternate Responsible Officials and Entity Official http://www.selectagents.gov/resources/APHIS-CDC_Form_1_Section_1A_1B.pdf.

- Name;
- Date of Birth;
- SSN;
- FBI UIN;[10]
- Supervising Principal Investigator;[11] and
- RO/ARO Signatures.

A hard copy of FSAP Form 1, for initial and amendment processing, is kept in the secured office of the PIADC RO. The retention period for this documentation is pending NARA's determination in 1.4 above.

The FSAP provides the unique identification number via fax to the RO/ARO who then enters the number into SAI. The FBI unique identification number is stored in the SAI system along with the name, date of birth, and SSN to account for the status of an individual's compliance requirements for access to select agents.

Information captured on the FBI CJIS FD-961, Bioterrorism Security Risk Assessment Form may include:

- FBI UIN;
- Legal Name (Alias(es));
- Date of Birth;
- SSN;
- Residence Address;
- Past States of Residence;
- Phone Number(s);
- Email Address(es);
- Gender;
- Ethnicity;
- Place of Birth;

[10] The FBI UIN is generated by the FBI and provided to the PIADC Select Agent Program after an applicant submits his or her FD-961 to the FBI as required to work in the Federal Select Agent Program.
[11] The Supervising Principal Investigator is the supervising scientist of the individual filling in the FSAP Form 1.

- Country or Countries of Citizenship;
- Alien Registration Number (A-Number);
- Immigration Status;
- Immigration Status at Entry;
- Date and Place of Entry;
- Parents' Names;
- Foreign Place of Birth Information, if applicable;
- Photo;
- Fingerprint image(s); and
- Certifications question(s).

The completed, original form, photo, and fingerprint images are forwarded to FBI CJIS via the PIADC Select Agent Program. S&T does not retain a copy of the completed form.

As a result of an approved risk assessment the following information is forwarded to PIADC by the FBI CJIS:

- SRA approval; and
- SRA date.

If an individual's risk assessment is not approved, the SRA approval and SRA date is not collected and a letter is sent letting the applicant know the reason for disapproval and appeal options.

Information captured on the PIADC General User Request Form, IT-007-1 may include:

- Name;
- Job Title;
- Organization;
- Office Phone;
- Office Address;
- Office Location;
- City and State;
- Employee Type (Government or Contractor); and

- U.S. Citizen.

A hard copy of the form is held by the IT department in the access-controlled Server Room. The retention period for this documentation is pending NARA's determination in 1.4 above.

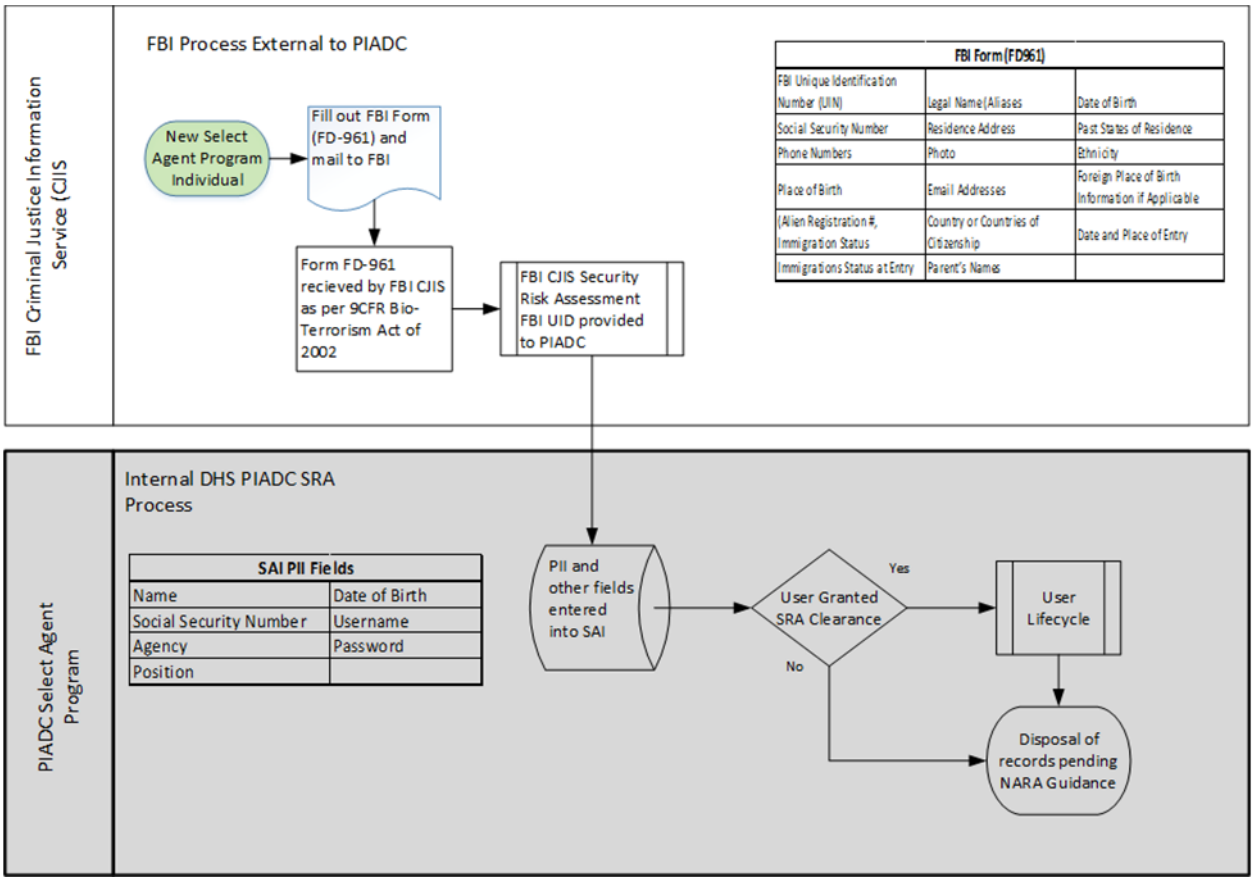
## 2.2 What are the sources of the information and how is the information collected for the project?

The individual provides the information necessary to populate the FBI CJIS, FSAP, and IT-007-1 forms.

The individual provides the information necessary to populate the FSAP Form 1. This information is also entered into SAI. PIADC sends the FSAP Form 1 to FSAP for processing, resulting in an FBI unique identifier number being returned to the PIADC RO/ARO for entry into SAI. SAI collects the name, date of birth, SSN, and FBI Unique Identification Number.

The individual fills in the FBI CJIS FD-961 Form and either hand delivers or mails it to the RO/ARO. The RO/ARO in turn mails the information required for the FBI CJIS FD-961 Form to the FBI. A risk assessment is conducted by FBI CJIS and this information is shared with PIADC through the FSAP and entered into SAI, which already holds the individual's information provided by the FSAP Form 1. PIADC only receives notification whether the individual passes or fails the risk assessment. The risk assessment is a background check based on the information provided in the FD-961. A letter is sent to the applicant letting him or her know the reason for failure and how he or she can appeal the decision by the Select Agent Program.

If the individual passes the risk assessment and is granted access to PIADC, the individual provides the information necessary to populate the PIADC General User Request Form, IT-007-1. Then the form is processed by the IT department and access is granted to SAI if appropriate. No data from the form is entered into SAI. A hard copy of the form is held in the facilities secured Server Room.




## 2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

## 2.4 Discuss how accuracy of the data is ensured.

The PIADC RO/AROs perform quarterly audits of SAI information and periodic audits of personnel information in SAI compared to the official report provided to PIADC by the Federal Select Agent Program listing individual's FBI Unique Identification Number, Name, Security Risk Assessment (SRA) status, and SRA expiration date. DHS also collects information directly from the individual, which increases the likelihood of accurate data.

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that PIADC is retaining more information in SAI than necessary to permit access to the facility.

**Mitigation:** PIADC works closely with staff from the DHS Office of the General Counsel, Security Office, Office of the Chief Information Security Officer, and Privacy Office to verify the data collected is within the scope of authorities established to secure the data. If the scope of authorities and data collection requirements change, PIADC will apply the updates to the data collections and remove any data that is no longer necessary or required. This PIA will be reviewed and updated as appropriate, should such a change occur.

**Privacy Risk:** There is a risk that there may be an unauthorized disclosure of the information.

**Mitigation:** While this risk can never be fully eliminated, SAI data (e.g., name, date of birth, SSN, FBI UIN, SRA approval, and SRA date) collected is located on a database server and uses current DHS information security software tools to lock down the system to ensure limited access to this information. System administrator(s), ROs, the information system security officer (ISSO), and DHS security personnel are the only users who have access to the system server. In addition, remote access is restricted.

## Section 3.0 Uses of the Information

### 3.1 Describe how and why the project uses the information.

PIADC and FBI personnel use the above PII/SPII to conduct a security risk assessment of individuals who require access to select agents and toxins, as required by federal statutes. The Federal Select Agent Program conducts risk assessments every three years. The FBI CJIS uses the information to conduct a background check on the individual and then returns the results of that check to PIADC. FBI CJIS requires SSNs for this collection because they provide the best matching capabilities to provide security risk assessments. The information is also used to conduct annual background checks.

### 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

### 3.3 Are there other components with assigned roles and responsibilities within the system?

No.

### 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** Unauthorized users may view the stored enrollment information or use the information for unauthorized purposes.

**Mitigation:** Only authorized personnel with a need-to-know will have access to the enrollment information. In addition to the system administrator, authorized personnel include the ISSO, ROs, and the security personnel. The ISSO accesses the system to conduct audits to ensure there is no suspicious activity or inappropriate use or access of the data. Security personnel will also have access to the information and the server system in order to operate the system. Access to the SAI will be restricted using user name and password protections.

## Section 4.0 Notice

### 4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

All registration forms for the Federal Select Agent Program include Privacy Act Statements describing the purpose for collection, use, and disclosure of the information.[12]

### 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All DHS federal employees and support contractors have a right to decline to provide information when requesting access for use of the SAI. If individuals decline to provide information they will not be processed for the enrollment portion, thus individuals will not be able to access the system.

### 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** Employees or contractors may be unaware that their information will be shared with the FBI.

**Mitigation:** Notice is provided to all individuals at the time of enrollment that includes background information on the system and its use as an additional measure of security for access control. The notice includes how the user's information is used and retained for use and an additional statement that cites S&T's legal authority to collect such information.

[12] http://www.selectagents.gov/resources/APHIS-CDC_Form_1_Guidance_Document.pdf

# Section 5.0 Data Retention by the project

## 5.1 Explain how long and for what reason the information is retained.

With regard to retention schedules and file plans for "Biological Select Agent and Toxins Records," these are currently unscheduled and with NARA for determination. DHS proposes to delete the records after 6 years. Until NARA approves the final retention schedule, the records are deemed permanent and cannot be destroyed. DHS deletes user access request information after 6 years pursuant to General Records Schedule 3.2 item 031.

## 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** SAI records are currently not covered by a NARA-approved records retention schedule, which means that the records are maintained longer than necessary for operations.

**Mitigation:** This risk is not mitigated. PIADC has submitted our Request for Records Disposition Authority to NARA and is following up with that office aggressively to resolve that issue. Until NARA acts, PIADC is not legally permitted to dispose of the records.

# Section 6.0 Information Sharing

## 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

End users of the system include staff from United States Department of Agriculture (USDA) Animal and Plant Health Inspection Service (APHIS) and Agricultural Research Service (ARS). PII used by PIADC in this process is forwarded to FBI CJIS for processing. Information is used to conduct background checks on personnel for access to SAI.

## 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Data is shared with the FBI to appropriately vet PIADC staff. DHS/ALL-023 Personnel Security Management SORN, Routine Use H permits DHS to share biographic information with an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a DHS decision concerning the issuance of a security clearance, the reporting of an investigation of an employee, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance

of the official duties of the person making the request.[13] Without checking with the FBI, DHS would be unable to meet the requirements of 9 CFR 121. Sharing of the relevant information with the FBI, facilitates the processing of clearances for individuals requesting access to select agents as required by 9 CFR 121.

### 6.3 Does the project place limitations on re-dissemination?

No. PIADC does not place any limitations on re-dissemination of the information. PII used by PIADC in this process is forwarded to FBI CJIS for processing and the FBI process sets limitations on how the information can be used. Data can be used pursuant to the Routine Uses listed in the System of Records Notices that cover this collection of information listed in section 1.2 and as described in sections V and VI on the FBI CJIS FD-961 Form.

### 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

PII used by PIADC in this process is forwarded to FBI CJIS for processing. As personnel submit their FBI CJIS FD-961 form for processing they are entered into SAI as pending. A report can be generated from SAI with a complete listing of cleared, terminated, and pending personnel as needed. This report reflects all disclosures of information to the FBI.

### 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** Information may be disclosed to external entities, and possibly used for unauthorized purposes.

**Mitigation:** PIADC only shares information in limited situations of supporting law enforcement investigations. PIADC shares information on a case by case basis, and in accordance with the DHS/ALL-023 Personnel Security Management SORN.[14]

## Section 7.0 Redress

### 7.1 What are the procedures that allow individuals to access their information?

Individuals can contact the RO or the Security Office if they wish to obtain access to their information. The contact information for the RO follows:

Science & Technology Directorate

[13] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010) *available at* www.dhs.gov/privacy.
[14] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010) *available at* www.dhs.gov/privacy.

Select Agent Program Manager, Responsible Official or Security Office
Plum Island Animal Disease Center
Phone: (631) 323-3200

Applicants seeking their personnel records may submit their request to the S&T Freedom of Information Act Office:

DHS S&T FOIA Officer
U.S. Department of Homeland Security, Science & Technology Directorate
Washington, D.C. 20528
Phone: 202-254-5700
E-mail: stfoia@hq.dhs.gov

The FASP conducts risk assessments every three years. Should an update or a need to change personal information arises prior to the renewal, that information is changed through a registration amendment and changed in SAI. An amendment is made by resubmission of a new Form 1 and submission to FSAP.

### 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals can contact the RO or the Security Office if they wish to obtain access to or correct their information.

### 7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals can contact the RO or the Security Office if they wish to obtain access to their information.

### 7.4 Privacy Impact Analysis: Related to Redress

There is no risk to redress because individuals have the opportunity to access and correct any inaccurate or erroneous information by working directly with the RO or the Security Office.

# Section 8.0 Auditing and Accountability

## 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Only the system administrators, ROs, ISSO, and security officers will have access to the information in SAI. The RO conducts semiannual audits of the listing provided by the Federal Select Agent Program by comparing the official program's list with what exists in the local database.

System administrators and security officers are required by DHS policies to abide by all privacy and information security regulations. The PIADC ISSO has access to the system to perform weekly audits.

## 8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All employees receive the DHS privacy and information security training annually. This is a mandatory requirement and the training records are maintained by the facility's human resources staff and the ISSO. In addition, PIADC requires a specific SAI training session previous to being provided access to the system.

## 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The SAI uses Active Directory to manage system accounts. Each account on the SAI is identified by a unique login account. Group logins are not allowed and are restricted within the confines of the software architecture.

The SAI is configured to only allow the System Administrator (SA) the privileges required to modify global account information, and as such are made aware by the ISSO that unique identifiers are required. Prior to a user gaining SAI access, he or she must complete a PIADC General User Request form, IT-007-1. Upon completion of the form, the user's supervisor signs the form validating the user's business justification for obtaining a SAI account. Upon gaining approval of the requesting user's supervisor, the form is submitted to the SAI SA for presentation to the System Owner. Once the SAI project supervisor approves the user's request, the user account is created and the user is required to sign the SAI Rules of Behavior prior to obtaining his or her logon credentials.

### 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

PII used by PIADC in this process is forwarded to FBI CJIS to identify those individuals who are prohibited from access to select agents and toxins based on the restrictions identified in the USA PATRIOT Act. New uses for the information or new access to the system would initially be processed through PIADC's change control process for our IT systems (and S&T CIO's if appropriate), the system owner, authorizing official, to the component Privacy Officer, and Associate General Counsel review.

## Responsible Official

Karon L. Floyd
Department of Homeland Security
Science & Technology Directorate
Plum Island Animal Disease Center
631-323-3200

Christopher S. Lee
Privacy Officer
Science & Technology Directorate
Department of Homeland Security

## Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security