Drug Enforcement Administration

Privacy Impact Assessment
for the
Academy Information System (ACADIS)

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Michelle Ramsden
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 12, 2025

(July 2023 DOJ PIA Template)

Section 1: Executive Summary

ACADIS is a commercial training management Information Technology (IT) system that automates many of the Drug Enforcement Administration (DEA) Office of Training's (TR) business processes. DEA uses ACADIS to request, schedule, and de-conflict the full range of DEA Training Academy processes. ACADIS accomplishes its purpose by providing TR with a centralized training management process contained in a single system where training schedules, lesson plans, and student records will be visible to employees with the requisite permissions. The system modernizes, unifies, and streamlines TR's workflow.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The mission of the Drug Enforcement Administration's (DEA) Office of Training (TR) is to develop, deliver and advocate preeminent law enforcement and non-law enforcement training to DEA personnel as well as appropriate federal, state, local, and foreign law enforcement counterparts. The function of the TR is to manage and coordinate all entry-level, advanced, special skills and leadership training programs for DEA Special Agents, Diversion Investigators, Chemists, Intelligence Research Specialists, and Sensitive Investigative Units. The DEA Academy in Quantico, Virgina, is the location where TR provides the initial training to Basic Agent Trainees, Basic Diversion Investigator Trainees, Basic Intelligence Research Specialist Trainees, and Basic Forensic Chemist Trainees. TR also manages and coordinates all supervisory/managerial and non-supervisory/non-managerial professional career development training (professional and executive development, certification programs) as well as core in-service, and specialized training programs within DEA. The ACADIS system assists with the TR's mission by providing a system to retain accurate and complete training history records.

ACADIS is a Commercial Off-The-Shelf (COTS) training management Information Technology (IT) system with the main purpose of serving as TR's main record keeping system including hosting most TR business processes and the academic records of trainees. ACADIS is a Software as a Service (SaaS), cloud-based platform utilizing Federal Risk and Authorization Management Program (FedRAMP)-Moderate authorized Amazon Web Services (AWS) GovCloud datacenter facilities via the service provider Vector Solutions. DEA has a contract with Vector Solutions who then contracts separately with AWS without involving DEA.

ACADIS end users are limited to DEA TR employees, however, basic trainees also have access to the ACADIS Portal, which is a module of ACADIS that allows them to complete online training, when assigned. Basic trainees do not have access to the ACADIS Production site where training records are held. DEA instructors and administrators use ACADIS to request, schedule, and de-conflict scheduling of a full range of DEA Training Academy resources, including facilities, conference rooms, classrooms, labs, instructors (who may be government employees or non-government

contractors), vehicles, firearms, and other training resources. Generally, except for completion of online training, trainees and graduates will not have direct access to the ACADIS system.

ACADIS also provides a training history for individuals who have received training and certifications, the instructors who provided the training, the curriculum the training was based on, and the qualifications and certifications granted so that they can be verified and, if necessary, established in court(if need to establish expertise). ACADIS uniquely identifies each user in accordance with Office of Personnel Management policy, which requires the collection and reporting of data concerning the completion of government-sponsored training for all federal employees. ACADIS also incorporates information for non-DEA employee instructors, speakers, or attendees to advanced in-service trainings or presentations. In fact, some attendees to in-service training events are individuals from state and local law enforcement agencies or foreign law enforcement partners.

ACADIS provides comprehensive, readily retrievable training records used for verification of training, for TR recordkeeping as well as litigation and agency Freedom of Information Act (FOIA) response purposes. ACADIS maintains accurate academic and certification records that can be positively identified, using Social Security numbers (SSNs), as belonging to specific individuals and can be accessed for proof of training, FOIAs, and litigation. ACADIS also maintains academic records throughout a learner's career in DEA government service in accordance with DEA standards for the retention and disposition of electronic records documented in the DEA Records Information System Handbook (DEARIS).

Other functions of ACADIS:

- The system supports the administering of TR testing, surveys, evaluations, and inventory management.
    - Written testing is accessed using a specific link and unique user ID provided by the exam proctor at the start of a test
    - Surveys are accessed using a specific link provided to trainees and responses are completely anonymous to all staff at TR
- Serves as the repository for records of review board actions that will result in decisions for the retention or dismissal of basic trainees.
- Facilitates the process of next of kin notification in the event of an individual's death or serious injury.
    - Next of kin contact information is provided by the individual at course convening and held on the individual's person record and accessed only by permissioned staff at TR.
- Promotes the creation of individual student biographies.
    - Information for student biographies is provided by the students using a webform that deposits their information into ACADIS without needing a unique login or other identifier. The information is held in a Webform repository until TR staff has reviewed and manually imported the data. The student has the opportunity to ask TR staff to edit their entries if desired.
- Contains instructor data, allows the assignment of instructors to scheduled offerings, and tracks instructor utilization.
- Supports being a repository for TR approved lesson plans.
- Facilitates the use of a field training program for graduates using conduct and performance evaluations post-entry to their first duty assignment.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	21 U.S.C § 801 *et seq*. (Controlled Substances Act) Section 2 of Public Law 85-507, The Government Employees Training Act of 1958. 5 U.S.C. § 4103 (Establishment of Training Programs) 44 U.S.C § 3301 *et seq*. (Federal Records Act of 1950)
Executive Order	Executive Order (E.O.) 11348: Providing for the Further Training of Government Employees E.O. 13111: Using Technology to Improve Training Opportunities for Federal Government Employees
Federal Regulation	5 C.F.R. § 410 – Training 28 C.F.R. §§ 0.100, 0.101
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	Names (First, last and middle initial) for DEA and other federal personnel or members of the public (US or Non-USPERs) are included in the system.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Date of birth or age	X	A, B, C, D	The date of birth or age of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) could be collected.
Place of birth			
Gender	X	A, B, C, D	Gender of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) could be collected.
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	SSN of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) are included in the system.
Tax Identification Number (TIN)			
Driver's license	X	A	Driver's License of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) could be collected.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	Personal mailing address of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) could be collected.
Personal e-mail address		A	Personal email addresses of DEA employees (Basic Agent students) could be collected.
Personal phone number	X	A, B, C, D	Personal Phone numbers of DEA employees, contractors, other federal government personnel, members of the public (US or non-USPERs) could be collected.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Education records	X	A, B, C, D	Education records of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) is be collected.
Military status or other information	X	A, B, C, D	Military status of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) could/would be collected.
Employment status, history, or similar information	X	A, B, C, D	Employment Status, history, etc. of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) is collected.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A	Conduct and performance ratings are generated and stored for post Basic Agent graduates (DEA Employees only).
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	Photos or photo identifiers of DEA employees, contractors, other federal government personnel, and members of the public (US or non-USPERs) could be collected.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	User IDs of DEA employees, contractors, and other federal government personnel are included in the system.
- **User passwords/codes**			
- **IP address**	X	A and B	IP address of DEA employees, contractors and other federal government personnel are included in the system.
- **Date/time of access**	X	A and B	Date/time of DEA employees, contractors and other federal government personnel are included in the system.
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	X
Phone		Email			

Other (specify):

NOTE: In person collection occurs only online using a direct link to a webform.

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the Component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			Personal Identity Verification (PIV) credentialed users only, accessible information is permissions based.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				*
Public				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			DEA counsel may request information on a case-by-case basis and any responsive information to subpoenas are provided by a credentialed and permissioned user in the Policy and Learning Development Section (TRP), Training and Development Unit (TRPT)
Private sector				
Foreign governments				*
Foreign entities				
Other (specify):				

NOTE: Records for State, local or foreign attendees to Academy presentations are not shared from ACADIS. Instead, in-service training attendees would be provided with certificates of completion at the end of the class/course attended.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Information in ACADIS will not be released for open data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The following Privacy Act statement will be used on the ACADIS System Access Request form to be signed by the individuals providing PII to record their consent. No other notice will be provided:

To receive access to ACADIS database complete and sign this form along with GS14 or higher supervisor signature. All account requests will receive an ACADIS Portal account and the below identified ACADIS Database accesses.

AUTHORITY: The Drug Enforcement Administration collects this information pursuant to:, "The Government Employees Training Act of 1958"; 5 U.S.C. § 4103, "Establishment of Training Programs"; Executive Order (E.O.) 11348 of Apr. 20, 1967, "Providing for the Further Training of Government Employees; E. O. 13111, "Using Technology to Improve Training Opportunities for Federal Government Employees." The authority for soliciting your Social Security Number (SSN) is E.O. 9397 "Numbering System for Federal Accounts Relating to Individual Persons", as amended by E.O. 13478.

PRINCIPAL PURPOSES: The DEA Office of Training (TR) collects this information in order to create user accounts and student profiles in "The Academy Information System" (ACADIS) Your Social Security Number (SSN) is needed to identify records unique to you.

ROUTINE USES: DEA may disclose these records in keeping with routine uses published in the federal register for the System of Records Notice JUSTICE/DEA-015, "Training Files," 52 Fed. Reg. 47182 (Dec. 11, 1987) (last published in full).

VOLUNTARINESS AND EFFECT: Although disclosure of your SSN or the other information requested is not mandatory, failure to disclose your SSN or the other information requested may delay or prevent your registration for training courses.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

This question is addressed in 5.1, above. If an individual refuses to provide information, DEA will not grant access to ACADIS.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)?

Individuals may gain access to information in the system pertaining to them via Freedom of Information Act or Privacy Act procedures. DOJ maintains procedures to process requests under the Privacy Act at 28 C.F.R. Part 16, Subpart D, Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974. For trainees, requests to change information in the system (i.e.- name changes, division and supervisor changes, etc.) are received through FIMService notifications and Access Management System notifications from DEA. However, trainees and graduates generally will not have direct access to this system, except for completion of on-line training.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ACADIS was granted authorization to operate on June 13, 2019 and expired December 31, 2022. This authorization will remain in effect until December 16, 2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
	This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: ACADIS was assigned the security category of Moderate as defined in FIPS-199 based on the aggregation of the information of several different and seemingly innocuous types of information (e.g. social security numbers, first/last name, etc.) together reveals sensitive information.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the DEA SCOP, or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.

X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** System logs are audited by the service provider in accordance with the System Security Plan Controls. Auditing/Accountability policies are reviewed every three (3) years and procedures are reviewed annually. All policies and procedures are reviewed if/when threat environments change are communicated to the service provider from the Joint Authorization Board/Authorizing Official (JAB/AO). The Cloud Services Provider (CSP) for the Software as a Service (SaaS) system, Vector Solutions, reviews all logs except inside the web application daily for anomalies; this includes logs at the Amazon Web Services (AWS) cloud networking layer, the application web server Windows logs, various supporting systems Linux logs, Oracle database logs, and other supporting application logs like antivirus. Vector Solutions also performs additional weekly and monthly higher-level reviews of logs and system performance data to review trends and identify anomalies for investigation and analysis. As a part of the FedRAMP cloud system certification program, the system undergoes a yearly audit by a third-party auditing organization (3PAO) which covers many core security controls related to access control and auditing. The System Administrator at DEA/TR reviews the auditing logs kept inside the application on a monthly basis. These logs record any user creation or deletion, role permissions changes, changes of user role assignments, exports of PII data, most deletions of data system-wide, and ad hoc querying of data.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Yes, as a standard operating procedure, all DEA contracts provide that contractors are bound by the Privacy Act, other applicable laws, DEA, and DOJ policy.
X	**Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Each component is required to implement foundational privacy training. The required training is distributed and tracked via the DOJ Learning Management System -DEALS. This training includes general mandatory annual training for information systems which include rules of behavior and cybersecurity Awareness Training that are applicable to DEA all component personnel. However, the Office of Chief Council (OCC) is working on a role-based annual privacy training which will be published soon.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII

in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Physical Controls:
Because ACADIS is web-based, all relevant Physical Controls to the actual system servers are maintained by Vector Solutions.

Technical Controls:
Built into the architecture of the system are standard encryption practices. These practices include encryption at rest for all storage based on AES-256 certificates and encryption in transmission using Transport Layer Security (TLS) 1.2 (again, based upon certificates using AES-256 cryptography). All encryption is also Federal Information Processing Standard (FIPS 140-2) approved.

Vector Solutions takes a "defense in depth" approach to security architecture in order to protect the confidentiality, integrity, and availability of ACADIS. This approach to security is designed to reduce the risk of external attacks. Backend infrastructure is completely segregated from front-end web servers using strict boundary protection and internal network segregation in accordance with SC-7. The Vector Solutions ACADIS web server provides data isolation/multitenancy so customer data is appropriately compartmentalized and secured. Vector Solutions employs Intrusion Detection System (IDS), file integrity monitoring, and real-time event logging and monitoring to ensure the ACADIS information security architecture is appropriately maintained. Vector Solutions only procures and deploys logical components if they meet strict security guidelines that reflect best practices as laid out in the information security architecture. The information security architecture is detailed in this SSP, which is reviewed and updated at least annually or whenever a significant change is made to the information system.

In accordance with Vector Solutions' defense-in-depth information security architecture, the ACADIS boundary meets this control through a combination of Network Access Control Lists (ACLs), host-based firewalls, IP whitelisting, and subnets. Vector Solutions utilizes Amazon CloudWatch for network monitoring capabilities at the external boundary. All internal network monitoring is conducted by Vector Solutions in accordance with SI-4. Vector Solutions is hosted within AWS GovCloud's data centers and uses their customer tenant services to define the ACADIS authorization boundary. The ACADIS system is completely logically separated from other customers hosted within AWS GovCloud's environment. The ACADIS tenant environment ensures that sensitive resources and data are completely isolated and secured. Vector Solutions uses subnets to separate customer-facing components and backend management components. Vector Solutions has implemented Network ACLs on the subnets to define the authorized traffic between subnets. The Network ACLs act as a firewall between the subnets to control traffic that flows in and out of the subnet. Vector Solutions has configured the Network ACLs with a deny-all, permit-by-exception methodology.

Vector Solutions considers all customer data to be categorized at the same sensitivity level, in accordance with the overall information system impact categorization as defined in the security control "Risk Categorization" (RA-2). There are many different types of information flows that are possible within the ACADIS system. Vector Solutions enforces external network boundary protection and internal network segregation policies in accordance with Vector Solutions defense-in-depth information security architecture. Authorized ports, protocols, and functions are strictly enforced, and sensitive information system components are prevented from communicating outside of the boundary

before first transiting closely controlled network interfaces, in accordance with security controls "Information Security Architecture" (PL-8) and "Boundary Protection" (SC-7). Finally, all external communications are encrypted to ensure transmission confidentiality and integrity, in accordance with "Transmission Confidentiality and Integrity" (SC-8).

Access Control for Transmission Medium is inherited from pre-existing FedRAMP Provisional Authorization to Operate for AWS GovCloud (US), 6/21/2016 (Transmission confidentiality and Integrity). Vector Solutions forces TLS 1.2 encryption for all external web traffic by redirecting all HTTP requests and only permitting inbound communication to the web interface via HTTPS. Additionally, all external connections to the Linux bastion host use SSH to establish secure tunnels.

Administrative Controls:
Access control policies are reviewed every three (3) years and procedures are reviewed annually. All applicable Access Controls are implemented and audited annually by a 3PAO via the service provider.

System access is restricted to single sign-on for all PIV users. Access to ACADIS is granted based upon need-to-know and least privilege principles. Access that has not been explicitly permitted is denied by default. Role-based access controls are employed to allocate logical access to a specific job function or area of responsibility.

System accounts are verified annually. All accounts requiring access to PII must be approved through the direct supervisor and the supervising GS-15. All accesses are promptly inactivated when user role-based requirements change. Only select personnel within the Office of Training are granted access to PII such as SSN and DOB.

Information governance is facilitated in ACADIS by utilizing existing features in the system. These features support information sharing by providing indications that the data users are viewing is special/protected. Additionally, permissions in ACADIS limit access to these identified records; ensuring that only authorized users have access to the data. Specifically, ACADIS supports identifying documents as containing restricted information, for example: PII. Documents with this setting selected then require special permission for users to access and view the data. Additionally, an icon will display to users indicating that it is a restricted document. The use of flags and tags within the ACADIS system also provides support for information sharing.

In order to protect customer data, Vector Solutions promulgates the Access Control and System Communication Protection policies to enforce information flow control within ACADIS at several levels, and implementing defense-in-depth information security architecture. AWS and its employees do not have access to DEA's instance of ACADIS. It is protected by encryption keys that are not accessible by AWS or any other agency. Defense-in-Depth is defined within the System Security and Privacy Plan required under NIST Special Publication 800-53, in controls PL-8 "Information Security Architecture" and SC-7 "Boundary Protection".

In addition, the Cloud Services Provider (CSP) for the SaaS system, Vector Solutions, conducts yearly Security Awareness training for its employees that includes curriculum that specifically teaches core privacy concepts and best practices that are used in the administration and support of the system.

Vector Solutions access control policy also ensures that all personnel that interact with the system, whether in a technical engineering capacity or directly supporting DEA from within the application, have passed a federal suitability clearance. Vector employees access the system by DEA System Administrator invitation only, and only for the purpose of performing live troubleshooting in company of the DEA System Administrator. Vector Solutions employees are given limited permissions to access only build-out components of the modules contained within the system (i.e. webforms, workflows, conduct and performance report templates). The System Administrator toggles Vector Solutions employee user status based on the need for access. All of these personnel are also individually authorized for access, and their access is reviewed on a periodic basis to verify that it is still required.

The System Administrators at the Office of Training conduct permission reviews of all assigned roles and account reviews of assigned roles on a monthly basis. The only option for downloading a report from the system is to save it to DEA's network infrastructure, Firebird.[1]

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Retention and disposition of electronic records contained in the Academy Information System (ACADIS) are administered in accordance with the DEA Records Information System Handbook (DEARIS), Enforcement Individual Training Files, Proficiency Test Files, File No. 810-02 (NC1-170-77-1). The disposition standards for the Federal records in these DEARIS are implemented in accordance with the NARA approved retention schedules. The length of document retention varies by the type of file it is:

- **File Number: 870-01 School Reporting Files**
  (e.g., trainee numbers/statistics, attendance, correspondence, etc.)
  These records are to be retained for TWO YEARS
- **File Number: 870-02 Individual Training Records Files**
  (e.g., records of grades, test scores, etc.)
  These records are to be retained for FIVE YEARS
- **File Number: 870-03 Proficiency Test Files**
  (e.g., weapons qualifications, Exercise, writing and presentation evaluations, etc.)
  These records are to be retained for THREE YEARS
- **File Number: 870-04 Record of Training Files**
  (e.g., forms relating to the course completion)
  These records to be retained: Review Annually. Destroy after employees leaves the DEA.

[1] Firebird is an on-premises/cloud hybrid, General Support System (GSS) environment that is the primary enterprise information technology (IT) application infrastructure of the DEA. Firebird provides network infrastructure to host multiple internally connected DEA information systems. The Firebird system will be covered by its own Privacy Impact Assessment.

- **File Number: 870-05 Law Officer Training Files (Basic Agent Trainees)**
  These records are to be retained for TWENTY-FIVE YEARS. Destroy after employees leaves the DEA
- **File Number: 870-06 Legal, Investigative, & Technical Training Files**
  (e.g., Basic Diversion Investigators, Forensic Chemist, and Intelligence Research Specialist Trainees)
  These records are to be retained for TEN YEARS. Destroy 10 years after date of document
- **File Number: 870-07 Foreign National Personnel Files**
- **File Number 870-08 Foreign Training Reporting Files**
  (Both 07 and 08 relate to selection, processing, and academic or progress reports of a Foreign National Trainee)
  These records are to be retained for THREE YEARS
- **File Number: 870-09 Administration of Technical Skills Training Files**
  (e.g., certifications, Trainings for HR, IT, Acquisitions, Budget, etc.)
  These records are to be retained for SIX YEARS
- **File Number: 870-10 Training Administration Files**
  (e.g., records documenting ancillary and administrative aspects of training)
  These records are to be retained for SIX YEARS
- **File Number: 870-11 Training Aids Files**
  (e.g., handouts. workbooks, instructional materials/lesson plans, videos, etc.)
  This document retention schedule applies to all of TR's programs:
  These records are to be retained for: PERMANENT
- **File Number: 870-12 Training Reporting Files**
  (e.g., records reflecting status of trainee, Trainee WebTA records)
  These records are to be retained for THREE YEARS
- **File Number: 870-13 Ethics Training Files**
  (e.g., rosters of those require to take ethics training, attendance, and training materials)
  These records are to be retained for SIX YEARS
- **File Number: 870-14 Non-Mission Related Training Program Files**
- **File Number: 870-15 Senior Executive Service Candidate Development Program (SESCDP)**
  (Both 14 and 15 mainly apply to SF-182 files)
  These records are to be retained for THREE YEARS (870-14) or per OPM regulations (870-15)

  NOTE: retention schedules may be affected/extended by litigation holds.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ___X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

DEA-015, *Training Files,* 52 Fed. Reg. 47217 (Dec. 11, 1987), as amended, https://www.justice.gov/opcl/docs/52fr47182.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

a. Potential Threats Related to Information Collection

Privacy Risk: Collecting and maintaining more personal information than necessary to accomplish DEA's official duties.

Mitigation: This risk is mitigated. ACADIS collects and maintains only that information about an individual that is relevant and necessary to accomplish system responsibilities. PII in ACADIS is obtained directly from the individual, either during the hiring process (for federal employees) or electronically when establishing a system account. No third parties are involved and the procedures for information collection are paperless. DEA ensures that ACADIS is able to:

- Uniquely identify each user in accordance with Office of Personnel Management policy, which requires the collection and reporting of data concerning the completion of government-sponsored training for all federal employees.
- Maintain accurate academic and certification records that can be positively identified, using Social Security Numbers (SSNs), as belonging to specific individuals and can be accessed for proof of training, FOIAs, and litigation. This academic record must be maintained throughout the individual's career in government service with the DEA, or as specified in the DEA Records Information System (DEARIS) handbook.
- Provide for positive identification of individuals who have received training and certifications, the instructors who provided the training, the curriculum the training was based on, and the qualifications and certifications granted so that they can be verified and, if necessary, established in court.
- Validate identity of individuals for the issuing of firearms, credentials, and badges.
- Support the creation of individual student biographies.
- Identify instructors, assign them to scheduled offerings, and track instructor utilization.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: Privacy threats arise from potential unauthorized access to and use of information in the system.

Mitigation: This risk is mitigated. Mitigation occurs through multiple privacy and security controls. The system is accessible only via DEA's Firebird information management system[2] which uses the PIV card for user identification and access control. Additionally, the system components that make up the ACADIS system are hosted within the AWS GovCloud datacenter facilities. DEA relies on GovCloud to provide appropriate physical and logical protections and processes for the AWS GovCloud datacenter facilities.

Further, system access is limited to DEA employees and contract personnel within TR, who have undergone background investigations. The System Administrator will limit and compartmentalize access to information within ACADIS by assigning users roles that will limit the scope of their read and write permissions based on duties and a demonstrated need to know. The following user groups will have access to the personnel records within ACADIS. System Administrators are contractors and training techs are both contractors and DEA employees.

Role	Description	Authorized by
System Administrator	Super user with full system access and authority to assign roles.	Section Chief TRP
Training Technician	Creates person records and schedules training. Assigns instructors, facilities, and training resources.	System Administrator
Unit or Section Chief	Oversees Unit Chiefs, instructors, Training Technicians, and trainees.	System Administrator

Note: The TRP Section Chief will always have System Administrator permissions because of the nature of the Training Unit, but other Section Chiefs will not (i.e. Diversion, Intel, etc.) and their permissions are managed by the System Administrator.

The Vendor Configuration Database Administrators will also have system access. These personnel have been cleared by DEA's Personnel Security Section at the unclassified level, which includes PII. They will have permission to execute Structured Query Language (SQL) and select queries that would afford them a technical ability to run SQL that displays PII in the results. This level of access is required for the vendor's configuration staff to be able to appropriately service and support the system.

As a FedRAMP authorized cloud computing solution, the vendor maintains the software and back-end database that comprise the ACADIS Readiness Suite. To maintain, troubleshoot, and upgrade this solution, Vector Solutions personnel must have administrator access to the database that houses DEA's ACADIS data. The vendor does not regularly read the data within the database but

[2] The Firebird system will be covered by its own Privacy Impact Assessment.

will do so as necessary when requested by DEA or for other types of trouble shooting. Inactive accounts will be inaccessible and can only be reactivated by the System Administrator.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: Potential risk that unauthorized individuals within DEA may access the system's PII or individuals outside DEA may receive PII from this system without a need to know.

Mitigation: This risk is mitigated. Access to ACADIS is not provided to other agencies and the information within ACADIS is not shared outside the agency. System access is restricted to single sign-on for all PIV users. Access to ACADIS is granted based upon need-to-know and least privilege principles. Access that has not been explicitly permitted is denied by default. Role-based access controls are employed to allocate logical access to a specific job function or area of responsibility. ACADIS information is not provided outside DEA except in certain carefully vetted circumstances and pursuant to an authorized exemption form the Privacy Act or routine use listed in a SORN.