Federal Bureau of Investigation

Privacy Impact Assessment
for the
Virtual Academy – Unclassified (VA-U)
Virtual Academy – Classified (VA-C)

Issued by:

Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: August 20, 2021

EXECUTIVE SUMMARY

The Virtual Academy is the Bureau's enterprise system for training and the repository for completed training records (i.e., training transcripts). The VA supports different types of training and training functions, including: course registration, approval, delivery (for online courseware[1]), transcript generation, and enterprise reporting. A VA Privacy Impact Assessment is being conducted, because VA collects and uses information in identifiable form that directly identifies individuals, including name, Social Security Number, and place of birth.

Section 1: Description of the Information System

(a) the purpose that the records and/or system are designed to serve

Virtual Academy is the completed training record system for the FBI. It also provides in-service course registration, online courseware delivery, classroom scheduling, Academy classroom scheduling, and enterprise reporting. The Virtual Academy (VA) system, owned by the Training Division of the FBI, provides the systematic delivery of training content and training management services to the entire FBI. The Virtual Academy system is composed of two separate systems, Virtual Academy Classified (VA-C) on the FBI Secret Enclave (FBISE) and the Virtual Academy Unclassified (VA-U) on the Azure Government (Gov) Cloud.[2] The primary difference between the two systems is the user population they support. The VA-C supports all FBI employees, contractors, and task force officers, while the VA-U supports all FBI's employees, contractors, task force officers and criminal justice partners (i.e., state, local, tribal, foreign, international law enforcement and intelligence partners). The VA-U provides the gateway to the National Academy Student Administration (NASA) component which houses application forms for class selection at the National Academy. Another function of VA-U is the use of online training courses by FBI law enforcement partners and US Intelligence Community personnel.

(b) the way the system operates to achieve the purpose(s)

Virtual Academy is constructed from a variety of commercial, off-the-shelf (COTS) and custom developed components, which are integrated in such a way that they appear to be a single application. The core component is the Learning Management System (LMS). The LMS contains the core functionality of the system, including: the course catalog, course registration, approval workflow, training progress data, and courseware management. However, the LMS alone cannot provide all the functionality required so other components have been purchased or developed to provide additional functionality. The Bureau Enterprise Training System (BETS) was developed to tie all the disparate components together, providing an easy to use interface to allow users to move seamlessly from one

[1] Courseware is a computer program or other material designed for use in an educational or training course.
[2] These enclaves (FBISE and Azure Gov Cloud) are covered by separate privacy documentation.

component to another.

The user interface for BETS is Virtual Academy's My Portal, the landing page for all Virtual Academy users. My Portal provides many useful features, including user selectable widgets, which are small, easily developed applets (a small application that performs one specific task) that provide specialized functions such as catalog search, quick links and announcements. BETS also provides the Navigation Bar, which provides useful links to all the most commonly used functions in the system and helps to tie everything together. BETS User Management is a custom developed application used to manage user accounts, organizations and roles. Other custom developed components include: Self-Reported Training (SRT), which allows users to report non-FBI sponsored training; Academy Dorm Registration System (ADRS), which supports dorm management at the National Academy; and NASA system, which supports a key Training Division program.

(c) the type of information collected, maintained, used, or disseminated by the system

Like any other enterprise information technology (IT) system, Virtual Academy must maintain enough user-related information to facilitate the system's use, including the tracking of training data that is subsequently created by user interaction with the system. The VA-C system therefore maintains information that is associated with all FBI employees and contractors who are required to interact with the system. Information in VA-C is demographic information imported from HR Source.[3] Individual training-related information, such as: online course completion data, and legacy system training data is maintained. The HR Source imported information is used to create VA-C user accounts and provide the VA system, to include VA-U, with the demographic information needed to manage those accounts.

Imported HR Source data consists of the following: first name, last name, middle initial, Social Security Number (SSN), place of birth, title, telephone number, fax number, date of birth, email address, career path, work specialty code, home state, home zip code, home phone, cost code, cost center name, division, section code, squad, Resident Agency (RA) code, RA name, organization title, job series, job family, where paid, where assigned, supervisor indicator, Entry on Duty (EOD), pay scale, pay grade, gender, file number, date assigned, and supervisor. Some of this information is collected to satisfy OPM reporting requirements. The VA-C retrieves HR Source data on a daily basis, via a database view. All VA-U and VA-C data is encrypted at rest and in-transit. Data-at-rest encryption is in place via managed AES 256 (secret key) disk encryption. The SSN is encrypted when inserted into the VA-C. The VA-C uses a database link over a secure connection to access the views provided by HR Source, on VA-C, and makes use of simple structured query language (SQL) queries to access the data in the views. The HR Source and VA-C have an Interface Control Document (ICD) explaining/outlining the agreed upon transfer process. The SSN is encrypted within the VA and used to uniquely identify users, but only encrypted forms of the SSN are compared. Users of VA, including enterprise applications, do not have access to the SSN attribute.

[3] HR Source is covered by separate privacy documentation.

Supervisor information is received from the WebTA system[4] every two weeks, via e-mail, and manually imported into the system. WebTA sends the VA database administrator (DBA) a file, via email on the FBI FBISE, of supervisor's SSN and subordinate's SSN, no other information is received. The DBA imports the file into the database, encrypting the SSN's during this process.

VA-U is also composed of COTS and custom developed components. Its primary purpose is to support all FBI employees, contractors and criminal justice partners by providing in-service course registration, online courseware delivery, classroom scheduling and National Academy registration. National Academy is a professional course of study available at the FBI Academy for U.S. and international law enforcement leaders that serves to improve the administration of justice in police departments and agencies in the United States and abroad by improving law enforcement standards, knowledge, and cooperation. VA-U maintains demographic and training-related information for individual law enforcement members as VA-C does for FBI employees and contractors, including online course progress, course completion and course registration information. VA-U uses roles similar to VA-C to control user access to individually identifiable information. VA-U data is stored on the Azure Government Cloud.

The VA-U collects and stores the following information in identifiable form that directly identifies individuals: first name, last name, middle initial, SSN (encrypted at rest), place of birth, title, telephone number, fax number, date of birth, email address, gender, nationality, and ethnicity. In addition, the following PII is collected from National Academy applicants: height, weight, residence, telephone number, residence email address, residence mailing address, and former addresses going back five years.

Full data-at-rest, and in-transit encryption, to include SSN's, is in place on the VA-C and VA-U via managed AES 256 disk encryption. The VA-C and VA-U fully encrypt all SSNs so they are not visible to any users, including application administrators. The Virtual Academy's underlying internal code immediately encrypts the SSNs upon importation from HR Source (for VA-C) and at the time of National Academy user registration (VA-U). From that point forward, the complete SSN will not be visible in any user interfaces or reports.

(d) who has access to information in the system

VA-C and VA-U are role-based systems; visibility of information to the user is based on the role that the system user has upon log-in. Each division has personnel who facilitate training within their respective organization, called personnel Organization Managers. In the Field Offices, these Organization Managers are Training Coordinators and Training Technicians, while in the Headquarters divisions, they are Training Officers. Organization Managers have full access to training records[5] associated with all individuals in their respective divisions. There are a limited number of users

[4] WebTA is covered by separate privacy documentation.
[5] "Training records" data is first name, middle initial, last name, title, division, job session, supervisor indicator, unique employee identification (UEID), course completion data (course taken), training completion date, training start date, training location, all elements of which are distinct from "user profile data."

(Enterprise Reporters and Power Users) with full access to training records associated with all individuals.

Below are the role assignments within the VA-C and VA-U system and the access/permissions associated with each role:

- **Student** – (aka "General Users") Users in this role have limited access to the system in order to request training, view content, see their transcript and take online training. Students only have access to their own basic profile, demographic data, and training records. They cannot view the training records of other students.
- **System Administrator** – Users in this role have access to all functions in the site, including system configuration functions (e.g., Categories, Organizations, and Email Addresses). They can also create, edit, and delete all course and content types and have access to run and manage all reports. They have access to view all training records and corresponding student's basic profile, extended profile, and demographic data. This role is a system role.
- **Program Owner** – (aka "Program Manager") Users in this role are assigned to specific programs and have access to completed training records. They can view student training records and corresponding user profile and demographic data,[6] but it is limited to training specific to their program.
- **Instructor** – Users in this role have the ability to manage students on their roster and their associated status (i.e., pass, fail) and set grades. Instructors have access to view the basic user profile and demographic data for students on their roster.
- **Class Coordinator** – Users in this role provide administrative support to Instructors for courses in the Virtual Academy and have the same access as the Instructor. Additionally, they act as the final approver for all classroom courses.
- **Organization Manager** – Users in this role include all Training Coordinators, Training Technicians and Training Officers. Users in this role have access to view training records, basic user profile, and demographic data for students within their organization only. They also process training requests for their Organization/Division.
- **Supervisor** – Users in this role have access to view the completed training records, basic user profile, and demographic data of all direct subordinates.

---

[6] "User profile data" consists of the following data fields: ID, login, full name, suffix, email, title, phone number, SSN, manager ID, input ID, input date, modified ID, modified date, organization ID, street address, fax number, profile (private), entry on duty, IS supervisor, job scale, job series, job grade, job family, career path, work specialty, gender, race, date of birth, file no., legacy ID, user type ID, registration status, actioning user, action date, denied comment, birth city, validated by ID, validated date, account status, RA code, RA name, career path stage, career path stage date, career path date, squad, supervisor code, cost code, cost center name, work specialty description, career path 2, career path date 2, career path stage 2, career path stage date 2, US citizen, alternate manager ID, HR system organization ID, functional title, privacy policy agreement, current agent EOD, last HR sync, parent status, last login date, HR sys UEID, last name in HR file, disabled by inactivity, BPMS status, work mobile phone, account disabled date, email verification required, lowered email, mobile number, user type name, date release notes viewed, home street address, home city, home state, home postal code, home country, full name LFM, HR Org. ID, building, room number, where working cost code, where assigned cost code, previous login, domain ID, education level ID, supervisor level code, supervisor level desc., profile readonly, Email UNET, Email SGOV., all elements of which are distinct from "training records" data.

- **Financial Manager** – Users in this role authorize expenditure of funds for courses/events. They do not have access to training records, user profile or student demographic data.
- **Chief Security Officer** – Users in this role have access to security related training data.
- **Course Manager** – Users in this role can add, edit, and delete courseware, curriculums, and tests. They do not have access to user training records nor profile/demographic data.
- **Enterprise Reporters** – Users in this role have access to view all training records along with corresponding basic user profile and demographic data in the system. Users in this role are limited to those with the need to access records enterprise-wide.
- **Component Administrators** – Users in these roles have access to all functions in the specific component (not system). They can create, edit, and delete all course and content types and have access to run and manage all reports for the component. (i.e., Universal Education Program (UEP), Event Request System (ERS), NASA, Program Management, Training Development and Delivery Plan (TDDP), Section Management (SM), and Mandatory Training Management (MTM)). Some components allow the administrator's access basic user profile, demographic data, as well as secured user profile data to manage their respective programs.

Data Categorization:

"Basic User Profile" can consist of the following data fields: first name, last name, middle name, full name, suffix, email, title, phone number, manager ID, organization name, fax number, entry on duty date, account status, registration status, current agent EOD, UEID, full name LFM, work mobile phone, mobile number, work street address, home street address, home city, home state, home postal code, home country, building, room number.

"Demographic Data" is used to categorize, group, aggregate and perform other analytic and reporting functions. This data consist of the following data fields: Is supervisor, race, job scale, job series, job grade, job family, career path, work specialty, gender, RA code, RA name, career path stage, career path stage date, career path date, squad, supervisor code, cost code, cost center name, work specialty description, career path 2, career path date 2, career path stage 2, career path stage date 2, US citizen, alternate manager ID, functional title, user type name, where working cost code, where assigned cost code, education level ID, supervisor level code, supervisor level desc.

"Extended User Profile" is additional user profile data not generally available to end users and used for the internal functioning of the system. This data consists of the following data fields: file no., legacy ID, user type ID, actioning user, action date, denied comment, validated by ID, validated date, HR system organization ID, privacy policy agreement, last HR sync, parent status, last login date, last name in HR file, disabled by inactivity, BPMS status, account disabled date, email verification required, lowered email, date release notes viewed, HR Org. ID, previous login, domain ID, profile read-only, Email UNET, Email SGOV.

"Secured User Profile" data is not generally visible to users of the application with the exception of system administrators and/or component administrators. This data can consist of the following fields: SSN, date of birth, birth city. Note: While SSN is available, it is an encrypted data field and access is severely restricted.

Physical access to the servers where information is stored is limited as the servers are physically located within secure, access-controlled data center locations.

(e) how information in the system is retrieved by the user

VA-C is Single Sign-On and accessible via the FBINet intranet. VA-U uses Single Sign-On when being accessed from the VA icon on the Law Enforcement Enterprise Portal (LEEP), which is a gateway for the law enforcement community to access multiple systems and services by using single sign on technology. VA-U is also accessible via the internet at https://fbiva.fbiacademy.edu, and users must sign on.

(f) how information is transmitted to and from the system

Virtual Academy 'data in transit' is encrypted via Transport Layer Security (TLS) from the 'user' via the Intranet on VA-C and Internet on VA-U to VA-C/VA-U IIS Web Application/Servers.

Demographic information is transferred to VA-C, on the secure network, from HR Source via a database link and secured in the VA. Individual training related information, such as online course completion data, and legacy system training data, is entered either by individual FBI employees for training provided outside of the FBI or automatically when the employee signs up and completes specific FBI online training. Supervisor information is received in VA-C from the WebTA system every two weeks, via e-mail, and manually imported into the systems.

Demographic information in VA-U is entered by authenticated, authorized individuals. Individual training related information is entered by authenticated, authorized individuals, by authorized instructors, or automatically when the individual signs up and completes specific FBI online training.

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The VA has agreements with several other FBI systems. There are no connections with non-FBI/DOJ systems. The FBI interfaces are documented in their respective Interface Control Documents (ICD). Below is a list of all the systems with which the VA currently has interfaces in place:

- Enterprise Process Automation System (EPAS)
- Human Resources Source (HR Source)
- Financial Reporting Application (FRA)
- Provisioning and Access Control (PAC)
- Unified Financial Management System (UFMS)[7]

[7] These systems (EPAS, HR Source, FRA, PAC, and UFMS) are covered by separate privacy documentation.

(h) whether it is a general support system, major application, or other type of system

VA is a FBI minor application that is not mission critical and is the Bureau's enterprise system for training and the repository for completed training records. VA is open to all users within the FBI and to other law enforcement personnel, but is a controlled, restricted application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID	X	Passport		Patient ID	
File/case ID		Credit card			

Other identifying numbers (specify): VA-C accounts are created using PII data received from HR Source. VA-C uses SSNs that are encrypted; not visible to any VA-C users, including application administrators. When displaying information on screen or in reports, the FBI Unique Employee Identification (UEID) is used in place of the SSN, this alleviates confusion between employees with the same last name.

VA-U only requires domestic law enforcement members who are applying to the National Academy program to enter their SSN. However, their SSN are masked to system administrators and National Academy Administrators in the user interface. Foreign nationals are uniquely identified using their first name, last name, birth city and birth state/country.

Per OPM regulation, the FBI provides a monthly bulk transfer of training data to DOJ. SSNs are required as a unique identifier. In order to minimize the risk of breach or receipt by an unauthorized individual, information is transmitted electronically via an encrypted connection.

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth	X	Financial info	

General personal data					
Alias		Home address	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age	X	Email address		Physical characteristics	
Race/ethnicity	X	Education	X	Mother's maiden name	

Other general personal data (specify): Home address, state, and zip code.

VA-C and VA-U also collect emergency contact information. This information, along with relationship between the student and the contact, will be collected in case of an emergency.

VA-U also collects emergency contact information of National Academy applicants. This information, along with relationship between the student and the contact, is collected in case of an emergency.

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	
Work address	X	Business associates			

Other work-related data (specify): Fax number, work specialty code, cost code for expenses, cost code for salary (if different), Division, Section, Squad, Resident Agency (RA) name and code, Organization, Job Series, Job Scale, Job Grade, Supervisor Indicator, Entry on Duty date (EOD), Career Path, pay scale, File number, Work Specialty and Date Assigned.

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

Other distinguishing features/biometrics (specify): N/A

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	

Other system/audit data (specify):

- Login and logout
- Creating, updating and deleting any content item (i.e., course hours or course description)
- Access approval requests
- Approval and denial actions
- Enrollment in a course

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

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

Other (specify): In order to uniquely identify a user, VA-C and VA-U requires a user to enter date of birth and city of birth, if this information is not already in the system.

VA-U will receive first/last name and email address from the VA-C which will allow users to associate their VA-U user account with their VA-C user account.

VA-U requires external Law Enforcement users to enter the following information online at registration:

- First name and last name
- Email address
- Phone number
- Agency/Organization

VA-U requires users applying for certain residency programs to enter the following additional information online at registration:

- Gender (required to assign dorm rooms)
- Nationality
- Address

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the

component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The improper or inappropriate access to PII, either unintentionally or on purpose, is the foremost privacy risk to be mitigated. Mitigation of this risk is managed using a multi-pronged approach. First is system access controlled. The VA-C has implemented a Single Sign-On (SSO) process that makes it very difficult for an individual to login as another user. This process uses the individual's network logon credentials to authenticate the user by validating them against the Secret Enclave Active Directory. Once validated, SSO then passes the credential through and creates an association between the user's Active Directory account and his or her Virtual Academy account. If the SSO process cannot match the account, it will then prompt the user for his or her SSN and use the SSN to enable SSO for the account. Once SSO is enabled, the user is automatically logged into the system from that point forward. Having SSO helps minimize the risk of someone logging into the system as a different individual because they would have to log into the FBISE as the user first, thus verifying they are an authorized FBISE user to start.

This privacy risk is also mitigated by the fact that full access to these databases is limited to a select group of users. Access is limited using roles that allow the system administrators to control access to information at the appropriate level.

In addition, VA-C collects certain information directly from the users in order to help facilitate the creation of various reports. For example, EOD information is used as a basis for career path training reports as well as for assignment of required training. The user's cost code allows users to be easily grouped for organization based reports.

The VA-U only requires SSNs from law enforcement members who apply to the National Academy program. Once a user's SSN is entered and saved to the system, it is immediately encrypted and the complete SSN is not visible to any system user. SSN are only kept for a limited period of time until it is no longer necessary for them to be maintained and then they are purged from the system in order to limit their exposure. This significantly reduces the number of SSNs maintained in the system at any given time.

The VA-U also collects emergency contact information of National Academy applicants (i.e., home address, state, and zip code). This information, along with relationship between the student and the contact, is collected in case of an emergency.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	X	For administering human resources programs
	For litigation		
X	Other (specify): For enterprise system for training and the repository for completed training records.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The information furnished to VA-C and VA-U is used to verify an individual's identity and provide an opportunity for training. It is necessary to have information about an individual's background and work experience in order to make sure he/she is obtaining appropriate and useful training, particularly with the collegiate level courses offered through the National Academy.[8]

Virtual Academy captures the information necessary to uniquely identify each user and the FBI sponsored training they are required to take, have requested, and/or have completed.

The information is collected and stored in order to allow Virtual Academy to perform several critical functions. These critical functions include:

- User Identification / Unique Identification – Virtual Academy must use information such as first name, middle name, last name, birth city,[9] date of birth and SSN. VA-U uses this information to vet potential National Academy students prior to arrival.
- Email Notification – Virtual Academy uses email notifications, which requires an email address for each user.
- Training Data Reporting – Virtual Academy contains a large amount of training-related data. Reporting against that data is of critical importance to the users of the VA system. In order to effectively generate reports, the following user information is maintained on the system: career path, work specialty code (used with a specific job series to indicate the specialty in which an individual works), cost code, cost center name, division, section code, squad, RA code, RA name, organization title, job series, job family, where paid, where assigned, supervisor indicator (supervisors have the ability to run reports of subordinates' training), EOD, pay scale, pay grade, gender, file number, and date assigned.

[8] Educational information is necessary to confirm an individual has an undergraduate degree prior to being allowed to take graduate level courses.

[9] Birth city is used when discrepancies arise between SSNs in the Active Directory and HR Source. Birth city is also used when SSNs are unavailable (i.e., with foreign nationals).

- Emergency Contact Notification – emergency contact information along with relationship is collected in case of an incident that requires making an emergency contact on behalf of the student.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	44 U.S.C. 3101; Government Employee Training Act, 5.U.S.C. 4101-4118
X	Executive Order	EO 11348 as amended by EO 12107
X	Federal Regulation	5 C.F.R. 410.311 and 5 C.F.R. 410.601
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

Records Management Division is still working with National Archives and Records Administration (NARA) to finalize a records retention schedule for the Virtual Academy. The proposed retention schedule divides training records into the following categories and retention periods.

For the Master file:

- **FBI Employees.** TEMPORARY. Transcript data can be deleted 25 years after deactivated.[10]

- **FBI-Sponsored personnel,** such as task force members, contractors, other government agency detailees, and interns). TEMPORARY. Delete information regarding FBI-provided and FBI-sponsored training 25 years after FBI sponsorship is deactivated.

- **External partners.** TEMPORARY. Delete information regarding training taken by members of external partners 25 years after the end of the calendar year in which a training course was completed.

For Outputs:

- Statistical Reports generated to justify staffing and resource allocations for personnel and support in order to fulfill training program priorities.

[10] If an FBI employee, after leaving the Bureau, then becomes employed by an external partner, the record of training that employee received while employed will be reactivated and managed under the guidelines of items (2) and (3) as appropriate.

Disposition: TEMPORARY. Delete/destroy when 10 years old, or no longer needed for analysis, whichever is later.

- Hotel Accommodation or Dormitory Assignment Reports. Delete reports when 2 years old, or when no longer needed after completion of the training session, whichever is sooner.

The project to finalize and implement these NARA requirements is still in progress. Until such time as the system is certified, the Records Management Division requires the Virtual Academy system to maintain all training records.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

PII Confidentiality Risk Level:

☐ **Low** ☑ **Moderate** ☐ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☑ **Yes: VA-C stores classified information.** ☑ **No: VA-U does not store classified information**
If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for

	matching PII access authorizations to access restrictions, such as contractual/MOU/ICD requirements.
X	Access Control for Mobile Devices: VA-U does not prohibit mobile access to reports, yet is secured by password and role authentication to the VA, and all SSN's are encrypted. VA-C access to PII is prohibited for Mobile Devices.

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access.
X	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 30-minute "time-out" functionality.

Media controls

	Media Access: access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted.
	Media Marking: media containing PII is labeled with distribution/handling caveats.
	Media Storage: media containing PII is securely stored.
	Media Transport: media is encrypted or stored in a locked container during transport.
	Media Sanitation: media is sanitized prior to re-use.
For Media Access, Marking, Storage, Transportation, and Sanitation, VA uses an unclassified, approved, FIPS 140-2 L3 encrypted thumb drive, which is labeled as such. The thumb drive is stored by the system administrator(s) onsite in a secured building. Transportation does not occur. Prior to media re-use, media will be completely sanitized with one of two methods: the eraser tool (FBI approved algorithm for securely erasing contents/files) or formatting (configuring process to delete data on hard disk or flash drives).	

Data Confidentiality controls

X	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
X	Protection of Information at Rest: information stored on a secondary storage device (e.g., hard drive or backup tape) is encrypted. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
For Transmission Confidentiality: data in transit is encrypted via TLS from the user to the web application/server. Data during transmission from HR Source and United Financial Management System (UFMS) to VA-C on the secret enclave is via a database link/view. SSN's are encrypted at rest. SSN's in the system are visible to Database Administrators (limited few), at the database level, via database query tools. VA-U data entry is secured by TLS and SSN's are encrypted at rest.	

Information System Monitoring

	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events
For Information System Monitoring, VA-C is working with Enterprise Security Operations Center (ESOC) and Secret – Cloud on Premise (S-COP) on the FBISE for a solution. The VA-U is monitored in-house by the Security Information and Event Management (SIEM) tool (i.e. Splunk) as well as the Azure Government Cloud which the VA-U is hosted on.	

Virtual Academy uses roles to control who has access to what information in the system. A small number of system administrators have access to most, but not all, PII maintained in the system. The exception is full SSNs for National Academy attendees, which are not visible within the application, but are stored in the database in encrypted form and only accessible to a limited select group. All PII maintained in the system is visible to Database Administrators at the database level via database query tools. However, the above access is very tightly controlled and only given to select personnel, all of whom are members of the Virtual Academy Unit. All FBI employees are required to take an online training course concerning the proper management of PII on annual basis.

Automatic purging of information in accordance with the retention schedule has not been implemented at this time but will be in the future once the schedule is finalized.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components		X		Per OPM regulation, the FBI provides a monthly bulk transfer to DOJ of all the training completions for the previous month.
Federal entities	X			Information in this system may be disclosed before a court or adjudicative body, in accordance with the relevant routine uses set forth in the system of records notices identified in Part 7.1.

State, local, tribal gov't entities			X	State and local entities are able to access information via a reports function pertaining to their personnel from their particular agency only.
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

Per OPM regulation, the FBI provides a monthly bulk transfer of training data, to include SSNs, to DOJ. In order to minimize the risk of breach or receipt by an unauthorized individual, information is transmitted electronically via an encrypted connection.

Disclosure of professional contact (i.e., FBI e-mail and phone number) and training (i.e., transcripts) information on VA-C and VA-U is limited to the role assignments noted under Section 1 (d) above with the exception of the NASA component. NASA applies to VA-U only.

Disclosure of professional contact (i.e., FBI e-mail and phone number) and training (i.e., transcripts) information on VA-U is limited to the role assignments noted under Section 1 (d) above, but unlike VA-C, VA-U may contain personal contact information for external law enforcement agencies, and criminal justice partner organizations. The ability to query contact (professional and personal) and training data via the Virtual Academy reports is restricted to only those personnel who are listed as Organization Managers or VA administrators.

Physical access to the servers where information is stored is limited as they are physically located within secure, access-controlled data center locations (i.e., the physical boundaries of the organization).

Incident Response is covered by the FBI Enterprise Cyber Security Incident Response Plan (ECSIRP). The ECSIRP is the incident reporting plan utilized for the Virtual Academy system administrators and

users. Data loss incidents, including the loss of PII, are required to be reported via the Security Incident Response System to the Chief Security Officer (CSO), Security Compliance Unit, and the FBI ESOC.

Access enforcement and authentication, on VA-C, is managed by the FBI's Active Directory. If a user is authenticated, credentials are trusted by the VA and the user is signed in using pass through authentication. Disabling a user account in AD will result in an SSO failure the next time the user attempts access. The VA-C user accounts are created based on the user's name being present in data from HR Source. The database contains the names of all FBI employees as well as all contractor employees who require access to FBI systems. If a name is not in the database after a VA account has previously been created, as is the case with an employee retirement, the VA-C user account is automatically disabled. Again, this is the case with a contractor employee whose security clearance has expired in the Facility Security System (FSS); their VA-C account will be disabled. HR Source and VA have an Interface Control Document (ICD) agreement.

Access enforcement and authentication has been automated to a great degree on the VA-U system. VA-U accounts are created based on the user's information being present in an XML data file exported from the VA-C and additional data entered manually by the user once authenticated and authorized by the initial login. The data export file contains the user account information of all FBI employees as well as all contractor employees who require access to FBI systems. If a name is not in the file after a VA-U account has previously been created (as in the case of employee retirement), then the VA-U user account is automatically disabled. This is also the case with a contractor employee whose security clearance has expired in FSS; their VA-C is disabled and in-turn their VA-U account will also be disabled. All other users will register for VA-U accounts manually, during which time enough information is collected to validate the user's request. Once submitted, the request must be approved by the agency's Training Manager, a Field Office Training Technician, or a VA System Administrator. Once approved, the user will be able to login on his own.

Separation of duties is implemented on VA-U and VA-C by using specific roles for System Administrators as well as many other application users such as User Managers, Class Coordinators, Schedulers and Program Managers.

Least Privilege is implemented on VA-U and VA-C by administering accounts on the basis of access to the role a user needs to perform their duties.

Audit Review, Analysis, and Reporting are performed on an as needed basis for VA-U and VA-C. All anomalies or deficiencies shall be reported to the VA Information System Security Officer (ISSO), Information System Security Representative (ISSR), Information System Security Manager (ISSM), and CSO.

All data in VA-C and VA-U is encrypted at-rest and in-transit.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected,

maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: The VA-U individual may decline to provide any of the information; however, if the person refuses, then he/she will not be provided access to the system or the training.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Although persons seeking to access VA-C may decline to provide information, because training and provision of such information may be a condition of employment, such declination may result in employment ineligibility or termination. No was checked here because of the very strong employment incentive to provide the information.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: The user consents to the use of his/her information for general training purposes as part of the registration process on the VA-C and VA-U. State, Local, and Tribal, Territorial employees have an opportunity to decline manually inputting certain profile data in VA-U. All VA-U users who decline consent to particular uses of information or who fail to complete their user profile may be denied access to training.

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Although persons seeking to access VA-C may seek to limit particular uses of their information, because particular uses of such information may be a condition of employment, such efforts to limit use may result in employment ineligibility or termination. "No" was checked here because of the very strong employment incentive to consent to all uses.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

FBI and other government agency employees are provided general notice of the existence of the training records system through publication of a number of system of records notices (SORNs) for the system. Specifically, the system relies on the Office of Personnel Management's SORN for federal employees, OPM-GOVT-1, for purposes of giving relevant federal employees notice on what information is collected from each user and how it will be used. The system also relies on the following SORNs for collecting, using, and maintaining non-federal employee records as it relates to accessing the FBI's facilities and DOJ computer systems, as well as facilitating and supporting internal and external collaboration and learning between the FBI and partners. These systems notices are reflected in the following: JUSTICE/FBI-002, "FBI Central Records System"; JUSTICE/DOJ-002 "DOJ Computer Systems Activity & Access Records"; and JUSTICE/FBI-004; "FBI Online Collaboration Systems."

Finally, all applicants to Virtual Academy are provided specific notice of the collection and use of individuals' information through relevant online or paper-based applicant forms. Individuals are also notified that failure to provide the requested information shall result in the denial of the application. A Privacy Act Notice is provided on both VA-U and VA-C.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.

X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: VA-C contains classified information and operates at the System Moderate Mode of Operation. For both VA-C and VA-U, the levels are Moderate for Confidentiality, Moderate for Integrity, and Low for Availability. Applicable security controls can be found in the System Security Plans located in the RiskVision system.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Audit logs are available and reviewed as needed, usually during system troubleshooting or when misuse is suspected. The logs are also reviewed as needed when performing evaluation of user access to the system.	
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: VA-C – AFU on S-COP 4/14/2018 VA-U – 3 year ATO (01/28-2020 to 01/26/2023) on the Azure Government Cloud	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Currently logon events are audited. Application administrators as well as role based and individuals are audited also.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component. Training is provided in the form of the application help system, job aides and demonstration videos which are available to all users.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

Technical safeguards to prevent misuse of data maintained in the Virtual Academy (VA-U and VA-C) include restrictions associated with every administrator account, role assignment, use of the FBISE's Rules of Behavior for all users and audit capabilities/reports within the system.

Role-based access helps to reduce the risk of unauthorized access or disclosure (Note Section 1 for VA role assignments within the system and corresponding associated access/permissions for each role).

Physical access to the servers where information is stored is limited as they are physically located within secure, access-controlled data center locations.

Access enforcement and authentication, on VA-C, is managed by the FBI's Active Directory. If a user is authenticated, credentials are trusted by the VA and the user is signed in using pass through authentication. Disabling a user account in AD will result in an SSO failure the next time the user attempts access. The VA-C user accounts are created based on the user's name being present in data from HR Source. The database contains the names of all FBI employees as well as all contractor employees who require access to FBI systems. If a name is not in the database after a VA account has previously been created, as is the case with an employee retirement, the VA-C user account is automatically disabled. Again, this is the case with a contractor employee whose security clearance has expired in FSS; their VA-C account will be disabled. HR Source and VA have an Interface Control Document agreement.

Access enforcement and authentication has been automated to a great degree on the VA-U system. VA-U accounts are created based on the user's information being present in an XML data file exported from the VA-C and additional data entered manually by the user during initial login. The data export file contains the user account information of all FBI employees as well as all contractor employees who require access to FBI systems. If a name is not in the file after a VA-U account has previously been created (as in the case of employee retirement) the VA-U user account is automatically disabled. This is also the case with a contractor employee whose security clearance has expired in FSS; their VA-C is disabled and in-turn their VA-U account will be disabled. All other users will register for VA-U accounts manually, during which time enough information is collected to validate the user's request. Once submitted, the request must be approved by the agencies Training Manager, a Field Office Training Technician or a VA System Administrator. Once approved, the user will be able to log in on their own.

Separation of duties is implemented on VA-U and VA-C by using specific roles for System Administrators as well as many other application users such as User Managers, Class Coordinators, Schedulers and Program Managers.

Least Privilege is implemented on VA-U and VA-C by administering accounts on the basis of access to the role a user needs to perform their duties. Audit Review, Analysis, and Reporting are performed on an as needed basis for VA-U and VA-C. All anomalies or deficiencies shall be reported to the VA ISSO, ISSR, ISSM, and the Training Division CSO.

Transmission confidentiality ('data in transit') is encrypted via TLS between the web client and the server for VA-U and VA-C. Data at rest (to include SSN's) is encrypted via AES 256 (secret key) encryption.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary

information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: Central Personnel Records, **OPM/GOVT-1**, 77 Fed. Reg. 73694 (Dec. 11, 2012), provides notice for training records about Federal employees (including contractors and volunteers). Non-Federal and Federal personnel are covered under FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 FR 24147 (May 25, 2017); DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); FBI Online Collaboration Systems, 82 Fed. Reg. 57291 (Dec. 4, 2017).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

To access information about a specific Virtual Academy user, a search is performed by a VA Administrator, based on the username or the user's last name and possibly the user's first name if needed for more common name searches. Searches can also be based on: division assignment, job title, job series, career path, and user type.