Privacy Impact Assessment
for the

Academy Class Management System (ACMS.net)

DHS/CBP/PIA-048

December 8, 2017

Contact Point

Mark A. Copanzzi
Director, Distance Learning Center
U.S. Customs and Border Protection
(304) 535-5437

Reviewing Official

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Customs and Border Protection (CBP) Office of Training and Development (OTD) administers the Academy Class Management System (ACMS.net) training management software program to track training and professional development. ACMS.net supports scheduling, skills, testing, registration, compliance, document management, graduation processing, Federal Law Enforcement Training Accreditation (FLETA) requirements, and attrition reporting. CBP is publishing this Privacy Impact Assessment (PIA) because ACMS.net collects, uses, and retains personally identifiable information (PII) about CBP personnel (employees and contractors) and employees from other Federal Government agencies.

Overview

The U.S. Customs and Border Protection (CBP) Office of Training and Development (OTD) coordinates and provides training to over 60,000 CBP personnel and contractors and other Federal Government agencies. CBP uses the Academy Class Management System (ACMS.net) for scheduling, skills, testing, registration, compliance, document management, graduation processing, Federal Law Enforcement Training Accreditation (FLETA) requirements,[1] and attrition reporting. ACMS.net was originally developed for the U.S. Border Patrol and has evolved into the consolidated student records, academy workflow automation, training management, and information tracking system. ACMS.net is used by all CBP training centers, facilities, and academies.

CBP also uses ACMS.net to record course completions, register students, generate transcripts, schedule instructors and resources, and facilitate overall class management. CBP developed ACMS.net to replace manual processes and local, stand-alone systems with a single, flexible management tool. ACMS.net consists of the following functions:

- **The Compliance Function** enables CBP to track and generate training certifications for students, organizations, and inventory; identifies conferral and renewal certification requirements; and monitors compliance to identify upcoming and recent expirations for students.
- **The Course Scheduling Function** provides the ability to build class schedules to support complex, multi-week training programs spread among multiple venues. ACMS.net automatically schedules instructors, facilities, and equipment based on existing resources and monitors scheduling conflicts across all training programs

[1] Federal Law Enforcement Training Accreditation (FLETA) has established and maintained a body of standards to promote the effective and efficient use of resources for federal law enforcement training. FLETA administers an accreditation process based on those standards to foster consistency in federal law enforcement training. For more information, please *see* https://www.fleta.gov/.

as well as identifies shortfalls and overages to optimize resource utilization. The system also has the ability to waitlist students based on existing class loads and memberships in an organization.

- **The Housing Management Function** enables CBP to automatically assign students to recommend housing and to track housing costs.
- **The Instructor Tracking and Scheduling Function** provides a mechanism for CBP to manage instructor availability, define maximum workloads for CBP instructors, and track CBP instructor certifications and levels of instruction (*i.e.*, lead, support, or mentor).
- **The Inventory Management Function** allows CBP to manage training-related inventory including vehicles, accountable property, bulk resources, weapons, and facilities and specific inventory information such as the type, serial number, and certifications. The system also provides CBP the ability to track the inventory chain of custody by assigning inventory to specific personnel, locations, and classes.
- **The Registration Function** enables authorized ACMS.net users to register for in-person and online courses, confirm availability of courses, verify prerequisites, and receive email notifications when registration status changes. This function also tracks and records user contact information and emergency contact information, and tracks supervisor information.
- **The Resource Scheduling Function** tracks and manages CBP training facilities, resources, and equipment availability; provides resolution of scheduling conflicts; and automatically sends email notifications to CBP instructors.
- **The Training Tracking Function** allows CBP to record and report student performance and progress during a course, scores, and a pass/fail checklist. CBP is also able to create and manage curriculum templates for standardized classes and generate automated reminders of training and certificate renewals that are sent to the student via email.
- **The Reporting Function** provides an audit trail for CBP to search multiple records and training hours for students and CBP instructors, and respond to training-related Freedom of Information Act (FOIA) requests. ACMS.net provides a reporting feature to track travel-related expenses and detailed travel information, produce training incident reports, security rights reports, and statistical reports as well as produce and print training transcripts.

ACMS.net mitigates privacy risks through security measures such as role-based access controls, system auditing, user training, and other safeguards built into the system. Role-based access within

ACMS.net ensures that only individuals who require access to information in order to perform their duties will be able to review and edit student information. The data within the system resides on a secure server within the CBP network. In order to ensure that information is secure, the system provides routine electronic audit results that are reviewed by the Information System Security Officer. CBP limits the collection of information in ACMS.net to only information that is necessary to carry out its training mission. ACMS.net collects, when possible, information directly from the student, or the sponsoring agency, and allows students the opportunity to correct information by providing students with access to their profile within the system.

When an outside agency submits a request for training, CBP approves the training slots based on availability. An authorized ACMS.net user enters information about the student; outside agencies do not have access to the system and an authorized CBP ACMS.net user will enter the student's information that the outside agency provides. For new students, the student or an authorized ACMS.net user builds a profile for the student containing basic information such as name, address, email address, organizational affiliation, and class. Students receive an email indicating they have been registered for a class and instructing them to provide additional registration information.

CBP Law Enforcement Officers, certain other employees, and certain temporary duty employees are required to attend training at the U.S. Federal Law Enforcement Training Centers (FLETC). Prior to submitting a request for FLETC training, CBP collects the trainee's biographic and contact information, along with his or her Social Security number (SSN), in ACMS.net and then transfers the information to FLETC's training system database, the Student Administration and Scheduling System (SASS).[2]

Section 1.0 Authorities and Other Requirements

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

CBP derives the authority to collect the information in ACMS.net from the Government Employees Training Act, 5 U.S.C. §§ 4101-4118, as implemented by Executive Order 11348 of April 20, 1969, *Providing for the Further Training of Government Employees*[3] and Title 20, section 422.103 of the Code of Federal Regulations as implemented by Executive Order 9397, and as amended by Executive Order 13478.

---

[2] *See* DHS/FLETC/PIA-002 Student Administration and Scheduling System (SASS), *available at* www.dhs.gov/privacy. FLETC requires the CBP Academies to collect the information from the CBP students (and Federal employees detailed to CBP) prior to referring them to FLETC for training. FLETC will not collect the student's information directly from the CBP employee.

[3] Executive Order 11348, *Providing for the Further Training of Government Employees, available at* https://www.archives.gov/federal-register/codification/executive-order/11348.html.

Executive Order 11348 requires agency heads to plan, program, budget, operate, and evaluate training programs for its own employees and extend such programs to other employees of other agencies whenever this results in better training, improved service, or savings to the Government. Executive Order 9397, as amended by Executive Order 13478, allows federal agencies to use an individual's SSN as a "permanent account number." The use of the SSN is made necessary because of the large number of present and former students who attend or have attended CBP programs, and who potentially may have identical names and dates of birth and whose identities can only be accurately distinguished by the SSN.

Finally, CBP derives its authority to collect the information in ACMS.net from its own inherent legal authorities for its employees to be trained in order for them to perform and effectuate CBP's law enforcement missions.

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

The student records contained in ACMS.net are covered by DHS/ALL-003 Department of Homeland Security General Training Records.[4] This SORN provides notice of CBP's maintenance of records associated with training. ACMS.net will collect and document training given to students who are provided CBP training. This system will provide CBP with a means to track the particular training that is provided, identify training trends and needs, monitor and track the expenditure of training and related travel funds, schedule training classes and programs, schedule instructors, track training items issued to students, assess the effectiveness of training, identify patterns, respond to requests for information related to the training of students, and facilitate the compilation of statistical information about training.

ACMS.net maintains emergency contact information for all students who are provided CBP training. Emergency contact information is covered under DHS/ALL-014 Personnel Emergency Contact Information System of Records.[5]

ACMS.net also provides CBP the ability to track the inventory chain of custody by assigning inventory to specific personnel, locations, and classes. This information is covered under DHS/ALL-010 Asset Management Records System of Records.[6]

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

The security plan is under development. The authority to operate is expected to be awarded

[4] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[5] DHS/ALL-014 Personnel Emergency Contact Information System of Records, 81 FR 48832 (August 25, 2016).
[6] DHS/ALL-010 Asset Management Records System of Records, 80 FR 58280 (September 28, 2015).

in November 2017 pending completion of this PIA.

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

The National Archives and Records Administration (NARA), General Records Schedule (GRS) 2.6 dictates the retention of employee training records. CBP is drafting a complete system schedule for ACMS.net, which is expected to align with the following guidelines:

- For any non-mission employee training records, ACMS.net will follow GRS 2.6 item 010, which are to be destroyed when three (3) years old or when superseded or obsolete.
- For law enforcement student training records, CBP has proposed a 40-year retention schedule (Disposition Authority Number DAA-0568-2017-0011-0002) to ensure that the records will remain retrievable throughout an employee's active career.[7]

Student records and training schedules are retained to validate the type, duration, and extent of training provided; to support any legal proceedings by producing the records in that designated timeframe; and to support any other CBP activities (budget, processes, government transactions, etc.) either by the CBP or other individuals linked to CBP such as the attorney general, or other legal entities that subpoena the records.

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

Personal information contained in the system is gathered from law enforcement agencies registering their employees as prospective CBP students, or from the students themselves, seeking training to perform their law enforcement mission and is not covered by the Paperwork Reduction Act.

[7] In accordance with NARA Transmittal No. 27 regarding GRS 2.6, Employee Training Records (January 2017), agencies must submit their own schedules for records associated with mission activities (including law enforcement) because the value of the records varies across mission sets. *See* https://www.archives.gov/files/records-mgmt/grs/grs02-6-faqs.pdf.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

ACMS.net collects, uses, disseminates, and maintains the following information:

- Name;
- Date of birth (CBP personnel only);
- Social Security number (SSN) (CBP personnel and temporary duty assigned employees (other Federal employees) only);
- Gender (CBP personnel only to provide housing accommodations);
- Hash IDs (CBP personnel only);[8]
- Verification of a valid driver's license (radio button option only to indicate verification; license number is not captured in the system) (CBP personnel only);
- Full home address (CBP personnel only);
- Agency;
- Position (CBP personnel only);
- Duty location (CBP personnel only);
- Emergency contact information (including name and phone number);
- Work email address;
- Telephone number(s);
- CBP course exam results; and
- Student transcripts.

CBP collects SSNs from CBP personnel and detailees from other Federal Government agencies supporting CBP in preparation for training provided by FLETC. The majority of CBP employees (including all Law Enforcement Officers) are required to attend training at FLETC, and SSNs are a required data element for the FLETC training system database, SASS.[9]

ACMS.net also collects non-PII data elements for other federal law enforcement personnel detailed to CBP and CBP personnel, such as the date the student entered on duty, travel information, dormitory assignment information, and assigned assets.

[8] Hash ID is an internal identification number assigned to CBP employees created using an algorithm based on the individual employee's Social Security number.
[9] *See* DHS/FLETC/PIA-002 Student Administration and Scheduling System (February 12, 2013), *available at* www.dhs.gov/privacy.

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

Only CBP personnel may obtain direct access to ACMS.net. The student or the other federal law enforcement agency provide the employee information via email or telephone and are registered by authorized CBP personnel. The data captured in the system is stored in the student personal records. ACMS.net system administrators manage the automatic email process that notifies students to confirm and update their information. In addition, the ACMS.net system administrators receive all CBP employee data from the U.S. Department of Agriculture (USDA) National Finance Center (NFC) approximately once a month to import information and manually update student person records with any changes to information on employment office, duty location, and job title.

Active students may take tests and receive results through ACMS.net. The system automatically scores tests upon completion and posts student grades to their records. All personal information within ACMS.net is directly input by CBP authorized ACMS.net users, students, or posted as an automated function of the system. Individuals are only authorized to view their own information, and supervisors may only view information related to their employees. The system does not receive information or data from another system.

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

No. All data is provided directly or indirectly by the student or is information pertaining to the student that is generated during the course of training.

2.4 Discuss how accuracy of the data is ensured.

Information within ACMS.net is either collected directly from the student or submitted via the sponsoring agency. In general, CBP relies on the sponsoring agency to provide accurate information on its employees and authorized CBP personnel complete the registration process for the sponsoring agency's student. ACMS.net administrators use information from the USDA NFC to ensure CBP employee records are accurate and current. If CBP becomes aware of any inaccurate information, CBP will contact the sponsoring agency points of contact to ensure the information is correct. Additionally, students are able to complete and correct their own data within the system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk of overcollection because ACMS.net uploads an extract of all CBP employee information from the USDA NFC, regardless of whether that

employee is enrolled in ACMS.net for training.

Mitigation: This risk is mitigated. To register for any class in ACMS.net, a prospective student must have a "person record" in ACMS.net. All new CBP employees will attend some sort of new employee orientation or basic training, and these programs are housed in ACMS; therefore a person record is required for every CBP employee. For existing employees, leadership training or advanced training per the employee's specialty are also housed in ACMS.net. ACMS.net has to store the entire file of a CBP employee to permit the employee the ability to self-register when he or she needs or desires to take training.

Privacy Risk: There is a privacy risk of overcollection because ACMS.net collects SSNs from CBP personnel and temporary duty assigned employees.

Mitigation: This risk cannot be mitigated, particularly because a) the Office of Personnel Management (OPM) still relies on the SSN as the unique identifier for federal employees and b) the FLETC Student Administration and Scheduling System[10] requires that all trainees submit their SSN for housing and class management while in Glynco, Georgia. CBP complies with this requirement since the majority of CBP employees attend FLETC training, but has requested that FLETC explore other options for student tracking to minimize the use of SSN.

CBP has developed an ACMS.net advanced data export that captures the SASS-required data. The data is exported to an Excel spreadsheet from ACMS.net, and the spreadsheet is then directly imported into SASS. Only approved CBP-personnel at FLETC academies have access to this feature.

Privacy Risk: There is a privacy risk of overcollection because the CBP academies and training centers may generate their own web forms for registration that may contain PII beyond the data elements listed above.

Mitigation: This risk is mitigated. During the development of this PIA, the CBP Privacy Office determined this risk could not be technically mitigated, therefore the Office of Training and Development issued guidance requiring all ACMS.net administrators in the field to limit PII on all web forms to the data elements above. This PIA is the governing document for PII permitted in the ACMS.net system. Any other data elements have been purged from the system, and no new fields will be permitted without review by the CBP Privacy Officer, and an update to this PIA.

Privacy Risk: There is a privacy risk that the information in ACMS.net may be inaccurate because it relies on the sponsoring agency to provide the data, rather than collecting it directly from the individual.

Mitigation: CBP mitigates this risk by collecting information directly from the student

[10] DHS/FLETC/PIA-002 Student Administration and Scheduling System (February 12, 2013), *available at* www.dhs.gov/privacy.

whenever possible. If CBP becomes aware of any inaccurate information, it may contact the sponsoring agency points of contact to ensure information is correct. Additionally, students are able to complete and correct their own data within the system.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CBP uses ACMS.net to record course completions, register students, generate transcripts, schedule instructors and resources, and facilitate overall class management. CBP uses ACMS.net to track and generate training certifications, schedule classes, manage housing for offsite trainings, permit student registration, track instructor course offerings, and generate reports.

On a monthly basis, ACMS.net imports the name, date of birth, gender, and SSN to accurately identify records relating to all CBP employees from the bi-weekly feed from the USDA NFC. CBP training is an employment requirement for many students, and their training results become part of the personnel records maintained by CBP. Use of the SSN allows for accurate matching with the student's permanent employment records.

CBP uses the personal and business contact information to communicate with the student before, during, and after training. Emergency contact information is only used by CBP supervisors in the event of an emergency.

Student performance data, including exam results, is recorded on a transcript and is used in virtually the same way as a college transcript. Student transcripts and education are routinely used to validate training and experience for job qualifications, college and university training credits, and establishing a student's knowledge base for a given situation in the law enforcement environment. Access to exam results are permission-restricted to students and those personnel who are responsible for ensuring grades are entered in the system (*e.g.*, course coordinators, training technicians).

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

ACMS.net does not use technology to locate a predictive pattern or anomaly. Queries only return reports CBP will use during the training process. These reports include student rosters, individual student reports, and assessment results. CBP may use data from system queries to evaluate the success of various training programs and determine patterns for successful completion based on student demographics such as age, gender, and experience. To remain objective in

evaluating program effectiveness, CBP depersonalizes the data through the removal of names, Hash IDs, SSNs, and email addresses. CBP only uses aggregate data in the system to evaluate and improve training programs and approaches.

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

No. Only CBP personnel can access ACMS.net, as the system resides within the CBP firewall. Although CBP may train personnel from outside agencies, neither those personnel nor their agencies can access ACMS.net.

3.4 Privacy Impact Analysis Related to the Uses of Information

Privacy Risk: There is a privacy risk that the use of student SSNs may increase exposure to identity theft or result in the mishandling of PII.

Mitigation: This risk is partially mitigated. ACMS.net users' roles and responsibilities determine whether they can access and view SSNs. System and domain administrators receive the highest access allowing them to view full SSNs; all other users receive truncated or masked access depending on the role. All administrators have access to SSNs, but a specialized role that masks SSNs is used when conducting training to prevent non-administrators from viewing SSNs.

Privacy Risk: There is a privacy risk that CBP will use the information it collects in ACMS.net for non-training purposes, inconsistent with the original purpose for collection.

Mitigation: CBP mitigates this risk through access controls, ACMS.net training, Standard Operating Procedures, and auditing. Only authorized CBP ACMS.net users may access the information. Individuals accessing or using the system for purposes other than what is required to administer training programs are restricted from accessing ACMS.net.

Privacy Risk: There is a privacy risk that users may gain unauthorized access to the system.

Mitigation: CBP mitigates this risk through internal application-level, role-based access control for access to specific ACMS.net functions. An ACMS.net user only has access to information based on his/her role. Access to privileged functions for enforcing system/application access is restricted to authorized system administrators. Auditing is enabled across all components of the system in order to monitor and verify appropriate privilege usage on the system.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

DHS/ALL-003 Department of Homeland Security General Training Records[11] and the publication of this PIA provide notice to the individual. Additionally, for CBP employees, there is the User Acceptance Policy that must be accepted the first time a user logs in to ACMS.net. A Privacy Act Statement is posted on ACMS.net to explain CBP's authorities to collect the information, the purpose, its routine uses, and any penalties for failure to provide the information.

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

The information ACMS.net collects and maintains is required for all students. The individual is also given the opportunity to decline to provide their information by not submitting their information for the training opportunity. For many job positions within CBP, training is a condition of employment, and therefore is mandatory.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals may not know that their information is in ACMS.net, or understand how ACMS.net uses their information, specifically the SSN.

Mitigation: ACMS.net mitigates this privacy risk by collecting registrant and applicant information directly from the individual, as frequently as possible. Additionally, ACMS.net provides notice through DHS/ALL-003 Department of Homeland Security General Training Records System and this PIA. A Privacy Act Statement is posted on ACMS.net to explain the purpose of the information, its routine uses, and any penalties for failure to provide the information. Non-CBP trainees whose agencies provide their information to CBP on their behalf do not have specific notice (aside from this PIA) that their information is in ACMS.net; however, they are likely aware that CBP requires biographic information in order to register them for and deliver training.

[11] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

In accordance with the proposed retention schedule, CBP retains student information for 40 years so as to remain retrievable throughout the active career of CBP personnel. CBP retains student records and training schedules to validate the type, duration, and extent of training provided. When CBP personnel separate from CBP or when the training program is no longer in use, the user profiles are deactivated and archived in ACMS.net. This information provides a mechanism to validate training and experience for purposes of qualifying for jobs, obtaining training credit with colleges and universities, and establishing a student's knowledge base for a given situation in the work environment.

ACMS.net retains SSN for several reasons. SSN is the only unique identifier that can be used to retrieve the individual's record. CBP needs to retain SSN to match records of students who come back for multiple programs over the lifetime of their career, and to ensure training records are available if called into question (*e.g.*, by an agency investigating an incident or during a legal proceeding). In addition, retaining SSN allows CBP to identify students in the event that they request copies of their training records for use when applying for other Federal Government positions, seeking credit for training received at CBP, and documenting service.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that, due to the fact that CBP does not yet have a NARA-approved retention schedule for law enforcement student training records, CBP will maintain the information collected for a longer period than is appropriate in order to comply with the Federal Records Act, which does not permit agencies to delete records without an approved retention schedule.

Mitigation: CBP has submitted to NARA its draft retention schedule for law enforcement training records, and expects the schedule to be approved and in place prior to any of the records reaching the 40-year cutoff.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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

Agencies outside of CBP do not have access to ACMS.net, and CBP does not routinely share ACMS.net information with outside agencies. They do, however, occasionally sponsor students for CBP training. When a non-CBP student graduates from a CBP training course, CBP provides the academic records directly to the student. The student may then share the information at his/her own discretion.

In general, CBP may share training information connected to the hiring or retention of an employee with the Office of Personnel Management, educational institutions, or training facilities to verify employee attendance and performance. Information may not be disclosed outside of the sharing outlined in DHS/ALL-003 Department of Homeland Security General Training Records, without the written permission of the individual or the CBP Privacy Office. CBP's sharing of training information aligns with the following routine uses from the General Training Records SORN:

> (H) To a federal, state, tribal, local, or foreign government agency or professional licensing authority in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance or status of a license, grant, or other benefit by the requesting entity, to the extent that the information is relevant and necessary to the requesting entity's decision on the matter;
>
> (I) To educational institutions or training facilities for purposes of enrollment and verification of employee attendance and performance; and
>
> (J) To the Equal Employment Opportunity Commission, Merit Systems Protection Board, Office of the Special Counsel, Federal Labor Relations Authority, or Office of Personnel Management or to arbitrators and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties.

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

As mentioned in Section 1.2, the system collects information related to CBP training programs; CBP only shares information in accordance with the SORN and for consistent purposes, including: employee development; career development; and any hearings or appeals related to the provision of training programs.

6.3 Does the project place limitations on re-dissemination?

Yes. Information may not be disclosed outside of the sharing outlined in DHS/ALL-003 Department of Homeland Security General Training Records[12] without the written permission of the individual or the CBP Privacy Office. For all other external sharing of information, CBP will either include a letter to the organization or execute an information sharing and access agreement such as a Memorandum of Understanding (MOU) with the external agency such as with another federal agency indicating that CBP's Privacy Act records provided or are being transferred for use pursuant to applicable routine uses and that further disclosure of the records is not permissible.

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

In general, CBP discloses information from ACMS.net directly to the record subject, pursuant to a request from a recent trainee or current CBP employee. In some cases, CBP may release ACMS.net information pursuant to a FOIA request. The ACMS.net reporting function provides an audit trail for CBP to search multiple records and training hours for students and CBP instructors, and respond to training-related FOIA requests.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that CBP may improperly disclose information contained within ACMS.net.

Mitigation: CBP mitigates this risk because ACMS.net is not connected to other systems to facilitate regular or bulk sharing. All information is shared on a case-by-case basis as authorized by law and CBP provides notice that the information may not be re-disseminated. CBP provides the academic records directly to the student upon his/her written request. The student may then share the information at his/her own discretion.

[12] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

A student may verify and update his or her information 1) through a telephone call to the appropriate ACMS.net system administrator; 2) by accessing his/her record electronically via ACMS.net and 3) by requests for access to the information contained in ACMS.net made to CBP's FOIA Office via FOIA online at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

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

ACMS.net provides the functionality for individuals to correct some information contained in their records. Since other federal agency personnel do not have direct access to ACMS.net, they must request assistance from CBP to view and correct their individual record. If there is particular data that cannot be corrected by CBP personnel, they must request in writing to their supervisors, training coordinators, or domain administrators that their records be updated. No action will be taken to correct a record without a written request and proof that the information in question is inaccurate. Information collected within ACMS.net may also be corrected by submitting a written Privacy Act request.

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

During the registration process for the initial and any future course in ACMS.net, the students are prompted to confirm their information and are given the opportunity to correct their information at that time.

Access to ACMS.net is restricted to CBP personnel only. Since non-CBP students do not have access to the system, CBP generates an attendance sheet for all students' review on the first day of class to ensure transparency. Students have the opportunity to correct their information at

that time.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that the individual may be unable to correct his/her information in ACMS.net.

Mitigation: CBP mitigates this risk by allowing an individual to correct his/her information: 1) through a telephone call to the appropriate local administrator or through the ACMS Help Desk (ACMS-HELPDESK@cbp.dhs.gov); 2) by accessing his/her record electronically through ACMS.net; and 3) by allowing access and correction through the procedures outlined in DHS/ALL-003 Department of Homeland Security General Training Records.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

In order to minimize or mitigate the risk of unnecessary or inappropriate use of information, ACMS.net uses the following controls:

- Database access must be requested through a supervisor;
- User names are assigned by the system;
- Access is role-based and determined by user profile;
- SSNs are entered upon initial registration, then masked within the system;
- Access to SSNs is tightly controlled;
- Student users are only able to access their own information;
- Only users with an official need to know, designated by the ACMS.net system administrator, will be able to access sensitive information once a student is registered; and
- Actions within ACMS.net are tracked automatically by the system via the Audit Trail Report.

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

All users must complete both an annual privacy and IT security-related training.

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

ACMS.net controls data access through data partitioning of domains and user roles. A domain defines the data a user can access; the role establishes what the user can do with that record in the database. Domain access and user roles are configured in the system according to the business requirements set forth by the ACMS.net Standard Operating Procedure. Access to ACMS.net falls in three general categories: (1) students; (2) ACMS.net administrative users (*e.g.*, training coordinators, training managers, instructors); and (3) system administrators including database administrators, network engineers, etc.

The ACMS.net system administrator grants access to ACMS.net administrative users at the request of the user's supervisor or contracting officer's representative. The request must specify the level of access required and verify the user's need-to-know. If approved, a profile is created and a role is assigned to the user.

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

CBP does not grant access to ACMS.net to outside users. For any information sharing arrangement, OTD would follow existing protocols and collaborate with the CBP Privacy and Diversity Office and the CBP Office of Chief Counsel.

Responsible Officials

Mark A. Copanzzi, Director
Distance Learning Center
U.S. Customs and Border Protection

Debra L. Danisek, CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security