Community Relations Service

Privacy Impact Assessment
for the
Adobe Connect Learning Management System

Issued by:

Antoinette Barksdale, General Counsel

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: 7/15/2022

Section 1: Executive Summary

The Community Relations Service (CRS) uses the Adobe Connect learning management system (LMS) to deliver virtual, self-paced training services to outside parties, including state, local, and tribal law enforcement officers and community leaders. CRS uses Adobe Connect to deliver services and proposes to use the LMS capabilities of this platform. CRS has existing licenses to use the LMS. The use of an LMS will enable CRS to deliver training services to a significantly larger audience than the agency's current training delivery methods, including in-person and virtual delivery. CRS prepared this Privacy Impact Assessment because the LMS collects the names and email addresses of participants for purposes of registration and tracking course completion. No other information is collected, and the information can be deleted at any time by the CRS system administrator.

Section 2: Purpose and Use of the Information Technology

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

The Adobe Connect learning management system collects names and email addresses of participants for the purposes of training registration. This information helps CRS to understand the number of participants who registered and completed a training course. This information is maintained on the Adobe cloud, which is FedRAMP certified, and will not be shared or disseminated outside of CRS.

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

Authority		Citation/Reference
X	Statute	Title X, Civil Rights Act of 1964 (as amended), 42 U.S.C., 2000-g-2b; Matthew Shephard and James Byrd, Jr. Act of 2009, 18 U.S.C., section 249
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	Names are collected for registration purposes
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Personal e-mail address	X	A, B, C, and D	Note: members of the public that register for CRS training programs are typically local and state public servants, like law enforcement officers. These individuals provide their work email addresses. Email addresses are collected for registration purposes.
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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

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

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

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

Section 4: Information Sharing

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

The names and email addresses collected from registrants will be shared within CRS only. The information is collected for internal tracking purposes and to provide training only. CRS will not share or disseminate the information to other agencies or components, or other non-governmental organizations.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			The information collected may be shared with component leadership and staff in positions with the necessary authorizations. Examples of sharing within CRS are sharing with the Deputy Director, General Counsel, and with conciliation specialists and program development in the field.
DOJ Components				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

No information will be made public for "open data" purposes.

Section 5: Notice, Consent, Access, and Amendment

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

CRS will notify individuals directly with a Privacy Act § 552a(e)(3) notice for individuals. Notice will be provided in the registration area of the LMS.

General notice has also been given that records maintained for the purpose of providing training to deliver virtual, self-paced training services to parties, including law enforcement officers and community leaders, are covered by JUSTICE/DOJ-002 "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24151, 153 (May 25, 2017). 86 Fed. Reg. 37188 (July 14, 2021).

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to

collection or specific uses of their information? If no opportunities, please explain why.

Individuals will voluntarily participate in CRS learning management system delivered trainings. If an individual chooses to not provide information to CRS to register for training, this may impact the individual's ability to participate in the training.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals have been notified that records maintained for the purpose of providing training to deliver virtual, self-paced training services to parties, including law enforcement officers and community leaders, can be accessed or amended in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-002 "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24151, 153 (May 25, 2017). 86 Fed. Reg. 37188 (July 14, 2021).

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** June 2022 **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DOJ OCIO will complete full authorization per Security and Privacy Assessment and Authorization (SPA&A) Handbook requirements for the use of Adobe Connect and LMS functionality.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Logs generated by CRS personnel are reviewed according to DOJ Cybersecurity

	Control standards. As this is a cloud-based SaaS system, DOJ can only review logs generated from CRS laptop use.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Privacy related training on the Adobe Connect learning management will be provided.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Training participant information collected by the Adobe Connect learning management system can only be accessed by CRS system administrators, including CRS employees and contractors with the necessary authorization. The number of CRS employees and contractors with administrative access is at least five total individuals. Each of these individuals have unique usernames and passwords and follow DOJ policy to maintain the security of this information. CRS employees with administrative authorization conduct periodic reviews of system logins to ensure that only authorized individuals are accessing the platform. All data and traffic from the DOJ network is encrypted, the cloud service provider provides data encryption at rest and in transit for their portion of the traffic flow.

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

The training registrant names and email addresses will be retained for a calendar year and then will be permanently deleted. However, this information can be deleted at anytime by an authorized system administrator.

Section 7: Privacy Act

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

_X____ No. _____ Yes.

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

In the event that records are retrieved in the future by a personal identifier, the applicable SORN is JUSTICE/DOJ-002 "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24151, 153 (May 25, 2017). 86 Fed. Reg. 37188 (July 14, 2021).

Section 8: Privacy Risks and Mitigation

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

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish CRS's official duties is always a potential threat to privacy. The LMS collects and maintains only information about an individual that is relevant and necessary to register users for training: the individual's name and email address. No other information is collected, and the information can be deleted at any time by the CRS system administrator.

b. Potential Threats Related to Use of the Information:

Potential threats to privacy as a result of CRS' use of the information in the LMS include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access, improper disposal of information, and/or unauthorized disclosure of the information.

The risk of unauthorized access is mitigated by 1) audits conducted by authorized CRS staff; 2) unique usernames and passwords for each system administrator; and 3) low number of individuals with administrative authorization. The risk of unauthorized individuals, including hackers, accessing the LMS is further mitigated by FedRAMP compliant security requirements and additional security controls implemented by Adobe.

Mandatory annual security awareness training for CRS personnel and contractors addresses the proper and safe handling of personally identifiable information (PII). Lastly, all CRS users are required on an annual basis to re-visit and comply with the DOJ Rules of Behavior which details the need to safeguard, protect and not misuse PII collected and maintained within the LMS.

c. Potential Threats Related to Dissemination

Security measures in place to safeguard sharing of information include: IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and system audit logs.

In addition, CRS has established minimum auditable events based on DOJ IT security requirements. The information system produces audit records, at a minimum that establish what type of event occurred, when and where it occurred, the source of the event, outcome of the event, and the identity of any user or subject associated with the event. The LMS does not transmit PII from this system to other internal systems, and other CRS systems cannot access PII housed within it, thereby eliminating the threat of inappropriate unauthorized access.

Consistent with FISMA and NIST security controls, CRS transmissions of PII occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), Secure Sockets Layer (SSL), or other encryption.