Privacy Impact Assessment

FMCS Institute System

Updated May 2024

Contact

Greg Goldstein

Senior Agency Official for Privacy

Federal Mediation & Conciliation Service

250 E Street SW

Washington, D.C. 20427

Privacy@fmcs.gov

Abstract

The E-Government Act of 2002, Section 208, and subsequent guidance from the Office of Management and Budget (OMB) establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII).

The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed.

The PIA ensures compliance with laws and regulations governing privacy and demonstrates the FMCS's commitment to protect the privacy of any personal information the agency collects, stores, retrieves, uses, and shares.

Overview

The Chief Learning Officer administer practical, experience-based, conflict resolution training for individuals and groups in the federal, public, and private sectors. These training courses involve conflict resolution, arbitration, and mediation courses specifically designed to meet the real-world challenges of labor-management relations. FMCS uses this system to register participants, provide accreditation information, and promote training and learning opportunities.

Section 1. Characterization of the Information

1.1 What information is collected, used, disseminated, created, or maintained in the system? Are the types of information collected, used, maintained, and /or shared specified in its privacy notices?

The FMCS Institute System collects, processes, and maintains participants' basic contact registration information to provide training and education services. This information includes:

- Full name;
- Full address including room number/mail code and country;
- Email Address;
- Title;
- Office and Organization name;
- Telephone and fax number;
- List of training programs;
- Course description;
- Instructor applicant information including education, background, and experience;
- Rosters;
- Course evaluations; and
- Registration details.

PII Mapping Components

FMCS Institute System consists of FMCS-00010 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the FMCS Institute System, FMCS-00010, and the functions that collect it are mapped below.

PII Mapped to Components				
Components	Does this function collect or store PII (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
Center for Conflict Resolution and Education (CCRE)	Yes	• Full name; • Full address including room number/mail code and country; • Email Address; • Title; • Office and Organization name; • Roster; • Telephone and fax number; and • Registration information.	To collect, process, and maintain participants' registration information to provide training, materials, updates, and education services.	FMCS buildings are guarded and monitored by 24 hour on-site professional security staff, cameras, ID checks, and other physical security measures; hard copy records are locked in a file storage area; and electronic records are stored in locations only accessible to authorize personnel requiring agency security credentials. Access to the system requires a username and password. FMCS administrators maintain access and accounts.

1.2 What are the sources of the information in the system?

The sources of information are provided by registrants through the online database registration program sponsored by FMCS. This includes information from applicants to be course instructors and course instructors providing information about education, background, and experience.

1.3 How is the information collected?

The information is primarily collected electronically from individuals registering for training or submitting applications to be a course instructor.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

The purpose of the information in the system is used for collecting, processing, and maintaining participants' basic contact registration information to provide training and education services. The registration information is required to provide training, accreditation information, and to help determine locations for agency resources. The system assists in processing the online registration of participants for the training activities.

1.5 How will this information be checked for accuracy?

The information is provided by the public. Therefore, the accuracy is ensured by collecting the information from the source, who must attest to the truthfulness and accuracy of the information they provide including any documentation.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

Federal Mediation and Conciliation Service, 29 U.S.C § 172, et seq., and 29 CFR part 1403.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Principle of Purpose Specification: The FMCS institute records should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose for which records, or data is intended to be used for.

Principle of Minimization: The FMCS should only collect PII that is directly relevant and necessary to accomplish its specified purposes and only retain PII for as long as necessary to fulfil its specified purposes. The PII should be disposed of in accordance with FMCS disposition schedules as approved by the National Archives and Records Administration (NARA).

Principle of Individual Participation: The FMCS involves the individual in the process of using or generating records. The agency also seeks individual consent for the collection, use, dissemination, and maintenance of PII.

Principle of Data Quality and Integrity: The FMCS ensures that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Risk Assessment: The main privacy concern is the identification of potential events that may negatively impact individual's contact information presented.

Privacy Risk**:** There is a privacy risk that the system will collect and maintain more information than is relevant and necessary to accomplish the agency's mission.

Mitigation: This risk is mitigated. FMCS will only collect information regarding the FMCS Institute records management system for processing and maintaining participants' basic contact registration

information to provide training, accreditation information, and to determine locations for agency resources which provides for a minimal collection of PII. Additionally, FMCS provides the statutory protections afforded under the Privacy Act, along with the privacy tenets in the Fair Information Practice Principles and strives to only collect personal information that is necessary to accomplish the agency's mission.

Section 2. Uses of the Information

2.1 Describe how the information in the system will be used in support of the program's business purpose?

The information in the system is used to promote training and learning opportunities concerning conflict resolution, arbitration, and mediation to the federal, public, and private sector employees which is part of the mission of FMCS.

2.2 What types of tools are used to analyzed data and what type of data may be produced?

There is not a special tool used to analyze the data. The reporting is simple, providing only a running total of individuals requesting information, an Excel spreadsheet. A report does not use PII but allows searching of requests by an assigned person responsible for solving and closing a request.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Access is determined by need. Need is determined by a user's ability to complete their tasks.

Are procedures, criteria, controls, and responsibilities regarding the access documented? All procedures, controls and responsibilities are documented and maintained in a secure location by the Office of Information Technology (IT). All hosted information is documented and managed by the Chief Learning Officer with assistance from IT.

Does access require manager approval? Yes, access is determined by job description and given with management approval.

Is access to the PII being monitored, tracked, or recorded? Yes, access to all records is monitored, tracked, or recorded.

IT is responsible for assuring safeguards and management of the internally stored information and internal information systems. All internal information systems are locked down, requiring strong authentication for access.

Principle of Transparency: Any information shared to the public is concise, easily accessible, easy to understand, and free from ambiguity and stated in plain language.

Principle of Use Limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law.

Risk Assessment: This ensures that the agency accurately measure and manage the risk associated with handling public information and keeps the agency compliant with the global or government data protection regulations.

Privacy Risk: The system will collect and maintain more information that is relevant and necessary to accomplish the agency's mission.

Mitigation: To mitigate this risk, only authorized users are allowed to access the records.

Section 3. Retention of Information

3.1 What information is being retained?

FMCS retains all information identified in Section 1.1.

3.2 How long is information retained?

All records are retained and disposed of in accordance with General Records Schedule (GRS) 6.5 issued by NARA.

3.3 Has the retention schedule been approved by the FMCS Records Office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule?

The retention schedule has been approved by the FMCS Records Office and NARA. The name of the record retention schedule is Public Customer Service Records, GRS 6.5, issued by NARA.

3.4 What are the procedures for the elimination of Sensitive Personal Information (SPI)?

Sensitive Personal Information (SPI) is minimized at the start by not asking for such information unless absolutely necessary to complete the system tasks. Additionally, information is protected by being kept on a secure server and limiting access to only those with need to know. Once the information has been used, it is removed from the servers so that public access is reduced or eliminated.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training?

The system is well designed to minimize the risk to privacy of using PII for research, testing, or training by adopting a protective and preventive mechanism to deprive unauthorized users by deploying several components including Event Espresso, emails, internal FMCS drives, and internal FMCS database requiring a username and password for system access**.**

3.6 PRIVACY IMPACT ASSESSMENT: Retention of Information

Principle of Minimization: The FMCS should only collect data or information that is directly relevant and necessary to accomplish the agency's purpose and only retain the information as long as necessary to support the system for its intended purpose. FMCS Institute records should be disposed of in accordance with GRS 6.5 issued by NARA.

Principle of Data Quality and Integrity: The FMCS Institute records should to the extent practical, ensure that PII is accurate, relevant, timely, and complete within the context of each use of the records.

Risk Assessment: This assists the agency to analyze and assess the privacy risks associated with the retention of records for individuals arising from the processing of their data.

Privacy Risk: There is a risk that unauthorized individuals may access the data for mischievous purposes which can lead to vicarious liability on the agency.

Mitigation: This risk is mitigated. The agency will take all reasonable steps necessary to maintain the security of all data collected, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure.

4.1 Which internal organizations is information shared or received? What information is shared or received, and for what purpose? How is the information transmitted or disclosed?

The internal organization which information is shared or received is the Chief Learning Officer. The information is collected, stored and shared in order to manage and conduct Institute courses and for future marketing purposes.

Information is transmitted or disclosed through the agency's internal drives, Event Espresso, Outlook, internal FMCS databases including the FMCS Institute records management system which are used to collect, process, and maintain participants' basic contact registration information, provide accreditation information, and provide training and education services.

The information FMCS shares or receives is listed in Section 1.1.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

There are various risks associated with the sharing of information within FMCS such as information security risks, compliance risks, and regulatory risks. Information security risk leads to data leakages and unwanted or unauthorized personnel having access to information. Compliance risk leads to failure to comply with laws, regulations, and standards. Regulatory risk leads to new regulations that threaten the agency business model.

What steps, if any, are currently being taken to mitigate those identified risks? The system is being assessed through agency internal drives requiring agency security credentials only accessible to limited authorized individuals in a need-to-know capacity.

Risk Assessment: This assists the agency to analyze and assess the privacy risks for individuals arising from the processing of their data.

Privacy Risk: There is a risk of sharing information with individuals without a valid need-to-know.

Mitigation: The centralization of data using a web application has mitigated most of the risks associated with the inadvertent release of information.

Section 5. External Sharing/Receiving and Disclosure

5.1 With which external organizations (outside FMCS) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FMCS as a routine use pursuant to 5 U.S.C. 552a(b)(3). The information FMCS shares/receives is listed in Section 1.1. The FMCS

Institute records management system is used to collect, process, and maintain participants' basic contact registration information to provide training and education services. The registration information is required to provide training, accreditation information, and to help determine locations for agency resources. The system assists in processing the online registration of participants for the training activities.

The FMCS Institute records may be received electronically and in hardcopy form from the public, federal, and private sector employees. The hardcopy forms are then scanned and stored electronically on FMCS servers for access for authorized personnel or users using their username and password.

Is sharing the information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of FMCS.

Yes, it is compatible with the original collection. It is also covered by an appropriate routine use in the SORN under 5 U.S.C 552a(b)(3) of the Privacy Act.

Describe how information is transmitted to entities external to FMCS and what security measures have been taken to protect it during transmission.

FMCS Institute records or information is transmitted electronically and is accessible to authorized personnel requiring agency security credentials. Access is restricted, and accessible to limited Human Resources and/or individuals in a need-to-know capacity. The Technical controls used on the system include a protected network developed by a trusted third-party contractor and only accessible to system administrators. The system is protected using a two-factor authentication log in system access. Also, the information must be transmitted on a secured network including Wi-Fi which will require a strong password to access the network and to prevent any unauthorized personnel or intruder in accessing the network.

External Sharing/Receiving and Disclosure				
Program Office or IT System information is shared/received with	Reason why information is shared/received with the specified program or IT System	List the specific information types that are shared/received with the Program or IT System	List all legal authority, binding agreement, SORN routine use, etc. that permit external sharing	Method of transmission and measures in place to secure data
Pursuant to the Privacy Act, all or a portion of the FMCS Institute records or information may be disclosed to authorized entities, as is determined to be relevant and necessary.	The information shared within the IT system is used to collect, process, and maintain participants' basic contact registration information to provide training and	Generally, FMCS Institute records or information is not shared externally unless generally permitted under 5 U.S.C. 552a(b) of the Privacy Act or	29 U.S.C § 172, et seq., and 29 CFR part 1403.	Records are stored electronically in locations accessible only to authorized FMCS personnel. Access is restricted only to individuals in a need-to-know capacity. The technical controls

	education services. The registration information is required to provide training, accreditation information, and to help determine locations for agency resources. The system assists in processing the online registration of participants for the training activities.	as a routine use pursuant to 5 U.S.C. 552a(b)(3).		used on the system include a protected network which is only accessible to system administrators. Transmission of data is done via secured email and/or authenticated data sharing via Microsoft platforms (OneDrive/SharePoint).

5.2 PRIVACY IMPACT ASSESSMENT: External Sharing/ Receiving and Disclosure

Risk Assessment: It is the identification of threat sources, vulnerabilities, and determination of the likelihood of occurrence to analyze and assess privacy risks for external sharing of information on individuals arising from the processing of their data and information.

Privacy Risk: There is a significant risk in sharing information outside the scope of the FMCS Institute Records SORN or without the authorized permission for disclosures. It can lead to violation of civil or criminal laws or regulations.

Mitigation: The risk is mitigated by ensuring FMCS Institute are only accessible to authorized personnel. Electronic records are stored on the agency's internal servers with restricted access to authorized personnel. Hard copy records are locked in a file storage area in FMCS buildings that are guarded and monitored by security personnel, cameras, and other physical security measures.

Section 6. Notice

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

Yes, there are Privacy Act Statements on forms and a system of records notice was published in the Federal Register. The system of records notice can be found here. The Privacy Act Statement on forms can be found here.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

Yes, individuals do have the opportunity or right to decline to provide information. Failure to provide the requested information could result in FMCS's delay or inability to provide services. To

receive training courses on conflict resolution, arbitration, and mediation services, and be provided accreditation information, individuals must provide basic information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes, as captured in the Privacy Act Statement on the form, individuals consent to the use of the information in accordance with the FMCS Institute Records SORN and as needed to receive training from FMCS.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Principle of Transparency: The FMCS is transparent and provide notice to individuals on the collection, use, dissemination, and maintenance of their FMCS Institute records or PII. The technologies or systems processing the FMCS Institute records and PII must be described in the FMCS Institute Records SORN.

Principle of Use Limitation: The agency uses FMCS Institute records and PII solely for the purposes specified in the notice.

Risk Assessment: This assists the agency to analyze and assess the risks in the notice provisions for individuals from the processing of their data.

Privacy Risk: There is a risk that individuals will not be given appropriate notice prior to the collection of their information.

Mitigation: The risk is mitigated at the outset of the collection process regarding the purpose of the collection, the routine uses of the disclosure of information, and the consequences for a failure to provide the information. The notice of the collection of information is provided through the PIA for the FMCS Institute Records, the Privacy Act Statement on forms, and the FMCS Institute Records SORN.

Section 7. Access, Redress, and Correction

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

Individuals must provide the following information for their records to be located and identified: (1) Full name, (2) Address, and (3) A reasonably identifying description of the record content requested. Requests can be submitted via fmcs.gov/foia/, via email to privacy@fmcs.gov, or via mail to FMCS, Privacy Office, 250 E Street, SW, Washington, D.C. 20427. For more information, see 29 CFR 1410.3, Individual access requests. Certificates of course completion may be requested via email to fmcs_institute@fmcs.gov.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Requests for correction or amendment of records may be submitted to the Privacy Office at privacy@fmcs.gov or via mail to FMCS, Privacy Office, 250 E Street, SW, Washington, D.C. 20427. For more information, visit https://www.fmcs.gov/privacy-policy/ and see 29 CFR 1410.6, requests for correction or amendment of records.

7.3 How are individuals notified of the procedures for correcting their information?

The PIA for the FMCS Institute SORN and the FMCS Institute SORN provides notice to individuals on how to correct their information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

There is formal redress provided for the correction of inaccurate information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, Redress, and Correction

Principle of Individual Participation: FMCS involves the individual in the process of using PII. FMCS seeks individual consent for the collection, use, dissemination, and maintenance of PII and provide mechanisms for appropriate access, correction, and redress regarding its use.

Risk Assessment: This assists the agency to analyze and assess the privacy risks for individuals in accessing, correcting, and redressing information.

Privacy Risk: An individual may not be aware of the process for assessing and/or correcting information.

Mitigation: To mitigate the risk, individuals may review the PIA for the FMCS Institute SORN and the FMCS Institute Records SORN.

Section 8. Technical Access and Security

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Users request access to the system and the Chief Learning Officer determines who needs access to the system, and in turn requests that access be provided to the user. Any users on the system must have valid FMCS credentials to log in to the system.

8.2 Will FMCS contractors have access to the system and the PII? If yes, what involvement will contactors have with design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, some contractors will have access to the system. Hosted systems are maintained by contractors. All contractors with access must have an NDA in place and a public trust background check completed. Any hosted systems meet government requirements for managing/maintaining/storing government data.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All FMCS users must undergo privacy awareness training and information security and awareness training before commencement of their job assignment. These trainings highlight the importance of securing FMCS information, PII, and information systems, identifies roles and responsibilities employees have when accessing agency systems, defines a privacy breach and how to report a breach, provide tips to avoid breaches in information security, provide the basics about the Privacy Act, and describes Privacy Act resources available at FMCS.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

The Institute system resides in several different FMCS systems, all of which have their own Authority to Operate (ATO). Our public website is hosted on Amazon Web Services (AWS) and holds its own ATO, including Event Espresso, the Institute system for registration. The remainder of the Institute system, including development and storage of training materials, reports and class information are maintained within Microsoft 365 (M365) including Exchange, SharePoint, OneDrive and Azure file shares. All of these locations are covered under the fully authorized FedRAMP ATO provided by Microsoft.