FMCS
FEDERAL MEDIATION &
CONCILIATION SERVICE

Privacy Impact Assessment

FMCS Conference System

September 20, 2022

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 ensures privacy issues have been identified and adequately addressed. The process is designed to guide FMCS system owners and developers in assessing privacy during the early stages of development and throughout the System Development Life Cycle (SDLC) to determine how the system will affect the privacy of individuals and the extent to which project objectives can be met while also protecting privacy. 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 and the Conflict Management Prevention (CMP)/International Office uses the Conference System to collect, develop, and maintain conference attendee and participation information in connection with FMCS conferences. The FMCS hosts, co-hosts, sponsors, or co-sponsors conferences designed to meet the real-world challenges of labor management relations, conflict resolution, mediation, and arbitration. The FMCS uses additional vendors to register attendees and participants and to promote conferences. FMCS uses GovDelivery Communications Cloud to promote conference and Cvent Conference Solutions (Cvent) to register attendees and participants for conferences.

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 collects basic information pertaining to individuals requesting to register for conference or conferences sponsored by the Agency. This information includes:

- List of conference programs, including event location, time, date, conference programs, and agendas;
- Information pertaining to registration, including names, registration fees, conference description, and professional affiliation;
- Attendee's information or participant information, including first name, last name, email address, title, office, employer/organization, address, room #/ mail code, city, state, zip/postal code, country, and telephone and fax number; and
- Information concerning the basis for and supporting documentation regarding the conference.

Yes, the information collected, used, maintained and/or shared in the system are specified in its privacy notices.

PII Mapping Components

FMCS Conference System consists of FMCS-00012 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FMCS Conference system, FMCS-00012, 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
The mapping of PII to components assist by linking of information type with non-PII or other specific information to identify an individual or entity. Participant contact information is captured by the Conference system.	Yes	• Full names • Email addresses • Title • Office • Employer/Organization • Full addresses • Telephone and fax numbers	The purpose of collecting information is to process and maintain a participant's or attendee's basic contact information for FMCS conferences. To coordinate delivering conference services, materials, and updates. The basic information is used to determine the participant’s or geographical location and to allocate Agency resources and have adequate preparation for the conference.	On FMCS premises, there is a NetApp Network attached Windows File System shared folder with permissions set to only allow those with designated access by membership thru a Windows Azure group membership. Group access and modification is controlled by IT which uses a privileged administrator account. Array is physically located in a locked computer room with limited badge access. Cvent and GovDelivery are remote hosted subscription systems accessed by username/password maintained by the host company and created by the user of the systems. FMCS administrators maintain accounts/access and content for the hosted spaces. Cvent and

				GovDelivery are both FedRAMP authorized vendors and use government accepted procedures for keeping data safe.

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

The sources of information generated or collected are from individuals requesting to register for or participate in an event sponsored by FMCS. The sources of information include attendees, speakers, exhibitors, officials, education professionals, FMCS employees, and guests.

1.3 How is the information collected?

The information is primarily collected via website from individuals requesting to register for an event sponsored by FMCS.

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

The purpose of the information is for FMCS to collect, process, and maintain participants’ or attendees’ basic contact information for FMCS conferences. The basic information is required to determine the participants’ or attendee’s regions or geographical locations and to have adequate preparation for the conference. This information is also used to assess the best allocation of FMCS resources.

1.5 How will this information be checked for accuracy?

The accuracy is ensured by collecting the information from the source who must attest to the truthfulness of the information provided, including any supporting documentation to support the registration of the program.

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

The FMCS is authorized to collect information under the following statutes: 29 U.S.C. 172; 29 U.S.C. 173 (e); and 29 C.F.R. 1403.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Principle of Purpose Specification: The FMCS conference records should mainly address 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: FMCS limits collection of personal information to what is directly relevant and necessary to accomplish its specified purposes and only retain PII for as long as necessary to fulfil its specified purposes. 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: FMCS protects personal data by adequate and reasonable security safeguards against such risks as loss or unauthorized access to data or information. FMCS also seeks individual consent for the collection, use, dissemination, and maintenance of PII.

Principle of Data Quality and Integrity: FMCS ensures the data or information collected is reliable and accurate i.e., the data is complete, consistent, and used for its intended purposes.

Risk Assessment: The main privacy concern is identifying potential activity 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 Conference Records System to process the conference attendee and participants' registration, to manage conference programs, and to collect information on FMCS's operations, 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 FMCS'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 shared in the system is used to process conference attendee's and participant registration. The information is used to promote the use of mediation, conflict resolution, and labor relations management in accordance with FMCS's mission through FMCS's participation in the conference. These conferences educate and train members of the public and private sectors. The other functions of this system include schedule setting, RSVP/Decline status, and outgoing messages from FMCS to attendees.

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

The GovDelivery is a web-based email subscription application, provided by Granicus, that allows members of the public to subscribe to receive information from FMCS via email for various conferences or educational opportunities. Also, Cvent, an on-line registration system, can handle conference registration, speaker information, and allow attendees to register online for any FMCS conferences.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Access is determined by need to know in order to complete their required tasks.

Are there procedures, criteria, controls, and responsibilities regarding the access documented? All conference records are stored on CVENT registration servers, which are FEDRAMP/FISMA compliant. Access to external systems is documented through host provider files and limited to individuals with need-to-know.

Does access require manager's approval? Yes, all access requires Conference leaderships' approval (usually the Chief Learning Officer or Manager of the Conflict Management Prevention (CMP)/International Office but could be other managers).

Is access to the PII being monitored, tracked, or recorded? All access to cloud hosted services is monitored and audited and can be accessed on request.

Who is responsible for the assuring of the safeguard for the PII? Cloud providers provide service-level agreements (SLAs) for safeguarding data. The owners of the data should be the ones responsible for safeguarding it.

Principle of Transparency: FMCS should be transparent in the use of individual data as stated or described in the SORN and PIA.

Principle of Use of Limitation: FMCS uses PII collected solely for the purposes specified.

Risk Assessment: It is the identification of threat sources, vulnerability of the system, and determination of the likelihood of occurrence of an event or activity amounting to risk.

Privacy Risk: There is a possible risk of misusing or mishandling collected information.

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

Section 3. Retention of Information

3.1 What information is being retained?

FMCS retains all information previously listed in section 1.1.

3.2 How long is information retained?

All records are retained and disposed of in accordance with General Records Schedule 6.4, issued by NARA and FMCS. Records are destroyed when three years old or when they are no longer needed for business use.

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 records retention schedule is Public Affairs Records.

3.4 What are the procedures for the elimination of Serial Peripheral Interface (SPI)?

The procedure for the elimination of SPI is adopting a common serial port with TX and RX lines called "Asynchronous." Asynchronous serial connections add extra start and stop bits to each byte which help the receiver sync up to data as it arrives.

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 of using PII by deploying Cloud-based services known as GovDelivery and Cvent and on premises there is a NetApp network attached Windows file system shared folder with permissions set to only allow those with designated access.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of Information

Principle of Minimization: FMCS should only collect PII that is directly relevant and necessary to accomplish the specified purposes and only retain PII for as long as necessary to fulfill the specified purposes. PII should be disposed of in accordance with FMCS records disposition schedules as approved by NARA.

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

Risk Assessment: The systematic way of evaluating the potential risk that is associated with the retention of records for individuals stemming from the processing of their data.

Privacy Risk: There is a possibility of retaining more information than necessary and retaining information longer than necessary.

Mitigation: FMCS applies NARA-approved records retention schedules to the information collected. Once the records meet the destruction date designated in GRS 6.4, FMCS will destroy the records upon three years or when they are no longer needed for business use.

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 are the Chief Learning Officer and CMP/International.

The information FMCS shares or receives is listed in Section 1.1. The purpose for the collection of information is for collecting, processing, and maintaining participant's or attendee's basic contact information for FMCS conferences. The basic information is required to determine the participant’s or attendee’s region or geographical location and to have adequate preparation for the conference. This information is used to assess the best allocation of FMCS resources and to perform the task.

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. The information security risk leads to data leakages and unwanted or unauthorized personnel having access to information. The compliance risk leads to failure to comply with laws, regulations, and standards. The regulatory risk leads to new regulations that threaten FMCS’s business model.

What steps, if any, are currently being taken to mitigate those identified risks? On FMCS premises, there is a NetApp Network attached Windows File system shared folder with permissions set to only allow those with designated access by membership thru a Windows Azure group membership.

Group access and modification is controlled by IT which uses a privileged administrator account. Array is physically located in a locked computer room with limited badge access.

The information is transmitted or shared through FMCS's internal servers with restricted access to only authorized personnel and designated officials as determined by agency officials.

Risk Assessment: This assists FMCS 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 NetApp Network has mitigated most of the risks associated with the inadvertent release of information. The most viable strategies are by deploying data encryption and strong and unique password for assessing of data in the system.

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 55a(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 determined to be relevant and necessary, outside the FMCS as a routine use pursuant to 5 U.S.C552a(b)(3). The information FMCS receives/shares is listed in section 1.1. The Conference System is used for collecting, processing, and maintaining participant's or attendee's basic contact information for FMCS conferences. The basic information is required to determine the participant's or attendee's region or geographical location and to have adequate preparation for the conference. The information is also used to assess the best allocation of FMCS resources. The system gives a detailed structure of the conference, including the conference program, keynote sessions, list of invited speakers with their background information, timetables for the conference meetings, venues of the conference, conference sponsors, and conference fees.

Registration records are held by CVENT on their hosted (FISMA/FedRAMP compliant) servers. FMCS then collects the information and download it to internal FMCS servers for reporting/conference use purposes. At all times, proper authentication via username/password is required for accessing the data, both internally and on hosted servers. Conference records are maintained in electronic form and only accessible to authorized personnel.

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.

GovDelivery is a web-based email subscription management application, powered by Granicus, that allow members of the public to subscribe to get information from FMCS via email. Cvent is an online registration system which can handle conference registration, speaker information, and allow attendees to register online for FMCS conferences. Cvent and GovDelivery are remote hosted subscription systems accessed by username/password maintained by the host company and created by the user of the systems. FMCS administrators maintain accounts/access and content for the hosted spaces. Cvent and GovDelivery are both FedRAMP authorized vendors and use government accepted procedures for keeping data safe.

The transmission of information or electronic records to external entities occurs through a web browser to the internet or from one of FMCS's hosted platforms. The information is transmitted securely using an encrypted protocol which require strong authentication for access.

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 Conference System 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 process and maintain records of individuals who participate in FMCS programs or activities who register for conferences or conferences sponsored by FMCS.	Generally, conference records or information is not shared externally unless generally permitted under 5 U.S.C. 552a(b) of the Privacy Act or as a routine use pursuant to 5 U.S.C. 552a(b)(3).	29 U.S.C. 172; 29 U.S.C. 173 (e); and 29 C.F.R. 1403	Records are stored electronically on FMCS's internal servers with restricted access to only authorized personnel and designated officials as determined by agency officials.

5.2 PRIVACY IMPACT ASSESSMENT: External Sharing/ Receiving and Disclosure

Risk Assessment: It is the identification of threat sources, vulnerabilities of the system, and determination of the likelihood of occurrence of activities that can impact FMCS.

Privacy Risk: There is a significant risk in sharing information outside the scope of the Conference 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 information is only accessible by authorized personnel. Electronic records are stored on FMCS's internal servers with restricted access to authorized personnel and designated officials as determined by agency policy.

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 notice 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 conference programs or registration confirmations, 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 Conference SORN and as needed to receive notifications on the programs and conferences from FMCS.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Principle of Transparency: FMCS provides notice to individuals regarding its collection, use, dissemination, and maintenance of PII or their conference records. The systems processing conference records and PII must be described in the Conference SORN.

Principle of Use Limitation: FMCS should not use or disclose personal information for purposes other than those which it has identified.

Risk Assessment: The identification of threat sources, vulnerabilities of the system, and determination of the likelihood of occurrence of activities and determining the impact of such risk to FMCS.

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

Mitigation: This risk is mitigated since the system provides notice at the onset 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. This risk is also mitigated since the notice of the collection of information is provided through the PIA available on the public facing website, the Privacy Act Statement on forms, and the systems of records notice in the *Federal Register* for the Conference SORN.

Section 7. Access, Redress, and Correction

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

Attendees and participants may access the GovDelivery system via links placed on client web pages or in system-generated emails. GovDelivery subscribers have access to their own personal data in the system. Cvent registrants may access their personal data through their registration confirmation or by contacting FMCS. 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, DC 20427. Also, see 29 CFR 1410.3, Individual access requests, for more information.

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

See 29 CFR 1410.6, Requests for correction or amendment of records, on how to contest the content of any records. Privacy Act requests to amend or correct records may be submitted to the Privacy Office at privacy@fmcs.gov or via mail to the Privacy Office at FMCS 250 E Street, SW Washington, D.C. 20427. Also, see https://www.fmcs.gov/privacy-policy/.

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

The PIA for Conference Records and the Conference 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: The identification of threat sources, vulnerabilities of the system, and determination of the likelihood of occurrence of activities and determining the impact of such risk to FMCS.

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

Mitigation: To mitigate the risk, FMCS has provided a PIA on our public facing website and provided a systems of records notice in the *Federal Regist*er so individuals are aware of the process for accessing and/or correcting information.

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?

All users are granted access on a need-to-know basis as determined by Senior Leadership and Senior Conference Officials. This process is determined and documented by Senior Leadership.

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, they will. All contractors accessing any of the systems associated with Conference records will have Non-Disclosure Agreements in place and will have gone through the security clearance process for a Public Trust clearance.

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?

Yes, for Microsoft Office 365 GCC5, Azure and eGovDelivery. Cvent is a FedRamp authorized product, so they meet federal security requirements, but we do not have an ATO with them beyond our procurement contract.