Privacy Impact Assessment

Survey 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

FMCS uses surveys to provide training and education, conduct interactive exercises, and create consensus during mediation and training meetings. For engagements with FMCS clients in meetings of all types, FMCS uses a collection of online engagement activity tools that includes SurveyMonkey, Poll Everywhere, Microsoft Forms, and FacilitatePro, all of which are online licensed software platforms, for customers' meeting effectiveness, electronic flip charting, project management, requests for assistance, event registration, needs assessments, and surveys. FMCS will use surveys from clients to evaluate services and employee performance.

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 system consists of records created or compiled during live training sessions and for purposes of evaluating FMCS's services. The system also includes FMCS employee and client responses to questions, surveys, and scenarios. These records include contact information for participants, and participant responses. System access records are also included (login information for users and FMCS staff). Specifically, these engagement programs might collect information names, participant responses to open-ended questions, contributions to a brainstorming activity in training or mediation, ideas that represent possible dispute resolution options, and other data. In short, the data that arrives through these engagement tools is the same or similar information that would be available to an FMCS mediator in any in-person meeting with clients and is handled with the same degree of confidentiality as a mediator would handle paper or traditional written data-gathering methods.

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

PII Mapping Components

The FMCS Survey System consists of FMCS-0002 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 Survey System, FMCS-0002, 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
• Office of Field Operations, Office of Education, and the Office of Client Services	Yes	• Full names • Email Address • Telephone No • Login information for users and FMCS staff	The purpose for the collection of basic information is to evaluate FMCS's services.	FMCS maintains the FacilitatePro data and user profiles on its own servers and have an electronic backup system in place in the event of a system failure, as well as an alternative system consistent with requirements of Continuing of Operations Plan. The system requires a username and password which can only be created by FMCS. FMCS employee access to these systems is on a limited license basis and requires use of internal agency network and drives. Access is restricted, and accessible to limited FMCS Personnel such as the Project Manager, System Administrator, IT, and/or individuals in a need-to-know capacity. The other platforms mentioned above are web-based programs and require either FMCS Office 365 credentials, usernames and passwords, or both, in order to be used by an employee of FMCS

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

The sources of information generated or collected are from FMCS clients or training registrants, conference attendees, and FMCS staff assigned to help process the survey results.

1.3 How is the information collected?

The information is primarily collected electronically using online engagement activity tools that includes Survey Monkey, Poll Everywhere, Microsoft Forms, and FacilitatePro.

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

The purpose of the information is to assess and evaluate the quality of services FMCS clients receive from FMCS.

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.

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: Federal Mediation and Conciliation Service, 29 U.S.C 172; et seq.; The National Labor Relations Act, 29 U.S.C. 151, et seq.; Administrative Dispute Resolution Act, 5 U.S.C. 571-584; Negotiated Rulemaking Act of 1990, 5 U.S.C. 561-570; the Federal Labor Relations Act, 5 U.S.C. 7119; and Departmental Regulations, 5 U.S.C. 301.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Principle of Purpose Specification: The FMCS survey 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 should limit 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. 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: 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 FMCS's mission.

Mitigation: This risk is mitigated. FMCS will only collect information regarding the Survey records system to evaluate FMCS's services. 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 for the purpose of assessing parties' needs, engaging parties to a dispute in finding resolution, collecting and handling data for use in negotiations and mediations, engaging parties in virtual meetings, teaching problem-solving skills, and creating and receiving evaluations from parties on the quality of services they receive from FMCS by collecting information used during live training sessions for educational purposes.

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

The FMCS uses a collection of online engagement activity tools that includes Survey Monkey, Poll Everywhere, Microsoft Forms, SharePoint, and FacilitatePro, all of which are online licensed software platforms for customer's meeting effectiveness, project management, electronic flip charting, request for assistance, event registration, needs assessments and surveys.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Management authorization is required for access. Login credentials and role assignments are only provided once authorization is received. To receive authorization, the user must have need-to-know for the specific survey/dataset and written justification.

Are procedures, criteria, controls, and responsibilities regarding the access documented? Yes, these are provided within the documentation of the system(s).

Does access require manager's approval? Yes, access requires manager's approval.

Is access to the PII being monitored, tracked, or recorded? Yes, access to PII is monitored, tracked, or recorded. Audit logs are maintained which include who accessed the system and when.

Who is responsible for assuring the safeguard for the PII? The Office of Information Technology is responsible for assuring safeguards and management of the internally stored information and

internal information systems. Responsibility for PII in cloud-based systems is held jointly by the Office of Information Technology and the Office of Client Services.

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 the 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 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 4.2, issued by NARA. Temporarily stored data or records received by the project manager are destroyed or deleted by the end of the fiscal year unless there is a specific need to retain it longer 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 Information Access and Protection Records, GRS 4.2.

3.4 What are the procedures for the elimination of SPI?

Sensitive Personal Information (SPI) The term "sensitive personal information", with respect to an individual, means any information about the individual maintained by an agency, including the following: (A) Education, financial transactions, medical history, and criminal or employment history. (B) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. To eliminate SPI, the system does not collect information irrelevant to the questions at hand. In addition, items that when combined could create SPI are kept separate from other data.

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 from accessing the system by using agency internal drives, an internal database which requires a

username and password, and web-based programs that require either FMCS Office 365 credentials, usernames and passwords, or both, in order to be used by an employee of FMCS.

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. The 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: This risk is mitigated. FMCS applies NARA-approved records retention schedules to the information collected. Temporarily stored data or records received by the project manager is deleted by the end of the fiscal year unless there is a specific need to retain it longer.

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

4.1 With 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 organizations which information is shared or received are the Office of Client Services, the Offices of Field Operations and the Director's Office.

The information is transmitted or disclosed securely via email, link sharing or paraphrased in reporting.

The information FMCS shares or receives is listed in Section 1.1. The survey records system is used to assess parties' needs, engage parties to a dispute in finding resolution, collect and handle data for use in negotiations and mediations, engage parties in virtual meetings, teach problem-solving skills, and create and receive evaluations from parties on the quality of services they receive from FMCS by collecting information used during live training sessions for educational purposes.

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 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 which require a username and password, an internal database which requires a username and password, and web-based programs that require either

FMCS Office 365 credentials, usernames and passwords, or both, for preventive measures to deprive unauthorized users from accessing records.

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 Survey records system is used to assess parties' needs, engage parties to a dispute in finding resolution, collect and handle data for use in negotiations and mediations, engage parties in virtual meetings, teach problem-solving skills, and create and receive evaluations from parties on the quality of services they receive from FMCS by collecting information used during live training sessions for educational purposes.

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?

Any information transmitted externally is done via secure email. The email is encrypted during transmission and is appropriately marked as 'CUI'.

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 Survey 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 assess parties' needs, engage parties to a dispute in finding resolution, collect and handle data for use in negotiations and mediations, engage parties in virtual meetings, teach problem-solving skills, and create and receive evaluations from parties on the quality of services they receive from FMCS by collecting information used during live training sessions for educational purposes.	Generally, Survey 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).	Federal Mediation and Conciliation Service, 29 U.S.C. 172, et seq.; The National Labor Relations Act, 29 U.S.C. 151, et seq.; Administrative Dispute Resolution Act, 5 U.S.C. 571-584; Negotiated Rulemaking Act of 1990, 5 U.S.C. 7119; and Departmental Regulations, 5 U.S.C. 301.	Any information transmitted externally is done via secure email. The email is encrypted during transmission and is appropriately marked as 'CUI'.

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 the agency.

Privacy Risk: There is a significant risk in sharing information outside the scope of the Survey 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 are only accessible by authorized personnel. Electronic records are stored on the agency's internal servers with restricted access to authorized personnel.

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 survey 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 surveys 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.

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 surveys, individuals consent to the use of the information in accordance with the Survey SORN.

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 survey records. The technologies and systems processing survey records and PII must be described in the Survey SORN.

Principle of Use Limitation: The agency 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 an agency.

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, and the notice in the Federal Register for the Survey SORN.

Section 7. Access, Redress, and Correction

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

FMCS employees, both current and former, may request access to their own records used as the basis for their performance evaluations through the Office of Human Resources. For external users, Privacy Act requests may be completed pursuant to 29 CFR 1410.3, Individual access requests. Individuals must provide the following information for their records to be located and identified: (1)

Full name, (2) Address, and (3) A specific description of the record content requested. Also, see https://www.fmcs.gov/privacy-policy/.

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 at Federal Mediation and Conciliation Service, 250 E Street, SW, Washington, DC 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 Survey records and the Survey 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 an agency.

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 notice in the *Federal Register,* 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?

Any users of the system must be vetted through management before any credentials and/or roles are assigned. Management shall determine if the user has need to access the system. This is documented in system documentation.

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?

It is possible that contractors may have access to the system. Any contractors accessing FMCS systems and information must be cleared at a minimum of Tier 2 Public Trust and have a signed NDA on file before receiving access.

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?

Each of the applications used within the Survey system have an Authorization to Operate statement on file with the Office of Information Technology (OIT) and filed with the Federal Risk and Authorization Management Program (FedRAMP®) Office as required.