FMCS | FEDERAL MEDIATION & CONCILIATION SERVICE

OFFICE OF GENERAL COUNSEL
PRIVACY IMPACT ASSESSMENT

The completion of FMCS PIAs is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002.

This PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phased of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing the privacy concerns during the development process, FMCS ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or under the Federal Information Security Management Act (FISMA).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Abstract

The overview provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Federal Mediation and Conciliation Service (FMCS) uses a system to collect, process, and maintain information from applicants who participate in the Shared Neutrals program as well as federal agency coordinators who request services from the program.

Overview

FMCS provides mediation service through the Shared Neutrals program to reduce the cost of litigation involving EEO and workplace disputes across all federal agencies. To properly provide service, information must be collected, maintained, created, used and disseminated as indicated below to achieve and fulfill its purpose.

Section 1. Characterization of the Information

Define the scope of the information requested and collected as well as the reasons for its collection as a part of the program, IT system or technology being developed.

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?

- Name of participant;
- Information pertaining to applicant to include position, associated agency, association with a Federal Executive Board, official duty station, and clearance level;
- Contact information to include physical location, phone numbers, and email addresses;
- Supervisor contact information;
- Request for accommodation information;
- Volunteer information to include cases, status, rank, and the number of hours volunteered for; and
- Other information related to case information, trainings attended, assessments from others, and general information about time in program and work outside of program.

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

PII Mapping Components

Shared Neutrals Records consists of FMCS-00011 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the Shared Neutrals Records and the functions that collect it are mapped below.

PII Mapped Components				
Components	Does this Component collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards for PII

OCS - SNU	Yes	Name Title Associated Agency Work address Email address Telephone number(s) Clearance level	To contact participants for trainings, notices of open cases and updates to the program. Also, to connect program participants with other federal employees to process cases.	Records are stored electronically in locations only accessible to authorize personnel requiring access. These records are secured and require multi-factor authentication to access.

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

Federal employees who wish to participate in the program submit their own information.

1.3 How is the information collected?

Federal employees who wish to participate in the program complete a survey (currently using Survey Monkey) for their PII to be placed on the training list. Federal employees who successfully complete the training submit a completed application form to sharedneutrals@fmcs.gov.

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

The purpose of the information being collected, used, maintained, and disseminated is to contact participants for trainings, notices of open cases and updates to the program. Also, to connect program participants with other federal employees to process cases.

1.5 How will this information be checked for accuracy?

Information is collected by the participant. For maintenance of accurate information, emails and use of a Form survey is used to request for updated contact information.

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 Departmental Regulations, 5 U.S.C. § 301.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential risks and what steps, if any, are currently being taken to mitigate those identified risks.

Principle of Purpose Specification: The FMCS Shared Neutral 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 Shared Neutrals System to process the Shared Neutrals attendee and participants' registration, to manage Shared Neutrals 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

Clearly delineate the use of information and the accuracy of the data being used.

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

The Shared Neutrals program is designed to coordinate federal employees with federal agencies in need of dispute resolution service. The purpose of the program is to reduce the cost of litigation involved in EEO and workplace disputes across all federal agencies. The purpose of the information is to organize and support agencies needing assistance from volunteer federal employee participants, to contact applicants and participants in the program, and to organize and analyze data for impact of service.

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

SharePoint and Microsoft Excel are used for data analysis. The type of data may include case information, mediator information and agency participation information.

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 criteria, procedures, controls, and responsibilities regarding access documented? All Shared Neutrals records are stored on FMCS shared drives or in SharePoint and the access is restricted. Access processes to shared drives and Microsoft shared services are documented and stored on the Information Technology (IT) restricted share or in Microsoft's documentation for their services.

Does access require manager approval? Yes, all access requires Shared Neutrals leadership's approval (usually the head of OCS 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 assuring safeguards for the PII? Cloud providers provide agreements (SLA's) for safeguarding data. The owners of the data are the ones responsible for safeguarding it from an Agency viewpoint. In this case, it would fall to the Office of Client Services to protect the data on cloud hosts. Any PII stored on FMCS servers would be protected by the FMCS IT Staff and FMCS policy for accessing FMCS data.

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 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

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is be being retained?

FMCS retains all information identified in 1.1

3.2 How long is information retained?

Names and contact information are retained for the length of time the participant remains in the program. Other records are retained and disposed of in accordance with the Agency's Records Schedule Approved 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)?

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 items such as 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 by deploying several components including emails, internal FMCS drives, and internal FMCS database requiring a username and password for system access.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risk associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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. Shared Neutrals records should be disposed of in accordance with GRS 6.5 issued by NARA and the Agency's Comprehensive Records Schedule approved by NARA.

Principle of Data Quality and Integrity: Shared Neutrals 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

The following questions are intended to define the scope of information sharing/receiving/transmitting within FMCS.

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

Information is shared and received by the Office of Client Services. The information is shared and received for processing requests and coordinating cases. Information is transmitted and disclosed through Forms, SharePoint,

Survey Monkey, Agency's internal drives, FMCS databases and emails. These "data systems" are subject to change consistent with Agency needs.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the risks associated with the sharing of information within FMCS (or the Department) and what steps, if any, are currently being taken to mitigate those identified risks.

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

The following questions are intended to define the content, scope, and authority for information sharing external to FMCS.

5.1 With which external organizations (outside FMCS) is information shared and received? What information is shared and received, and for what purpose?

Any federal agency requesting a Shared Neutral service or any federal employee providing a service to the requesting federal agency will receive relevant contact information to process case.

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.

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.

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

Information is emailed to the individuals involved in the case. These emails are secured in Exchange Online using Microsoft Government Community Cloud (GCC) processes.

External Sharing/Receiving and Disclosure				
Program Office or the IT System information is shared/received with	**Reason why information is shared/received with the specified Program Office or IT System**	**List what information is shared/received with the Program Office or IT System**	**List the legal authority, agreement, SORN routine use, etc. that permit external sharing/receiving**	**Method of Transmission and measures in place to secure information**
Any federal agency pertinent to the case.	To connect requesting federal agency with service of a federal employee.	Federal employee name and email are provided via email to federal agency requesting service. The name and email of the federal employee requesting service is provided to the federal employee providing service.	Federal Mediation and Conciliation Service, 29 U.S.C. 172, et seq., and Departmental Regulations, 5 U.S.C. § 301; and see SORN routine uses.	Information is emailed to the individuals involved in the case. These emails are secured in Exchange Online using Microsoft Government Community Cloud (GCC) processes.

5.2 PRIVACY IMPACT ASSESSMENT: External Sharing/Receiving and Disclosure

Discuss the privacy risks associated with the sharing of information outside FMCS and what steps, if any, are currently being taken to mitigate those identified risks.

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 risk in sharing information outside the scope of the Shared Neutrals System 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 Shared Neutrals records are only accessible to authorized personnel. Electronic records are stored on Microsoft cloud servers with access restricted to authorized personnel.

Section 6. Notice

The following questions are directed at providing notice to the individual of the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

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 and 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 there a penalty?

Individuals have a right to decline providing information, but if individuals do not provide the information requested, service cannot be provided, and the individual will not have the ability to participate in the program.

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 Shared Neutrals records.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe potential risks associated with insufficient notice and what steps, if any are currently being taken to mitigate identified risks.

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

Principle of Use Limitation: The Agency uses Shared Neutrals 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 Shared Neutrals, the Privacy Act Statement on forms, and the Shared Neutrals SORN.

Section 7. Access, Redress, and Correction

The following questions explore an individual's ability to ensure the accuracy of the information collected.

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

Individuals wishing to request access to their records should contact the Office of General Counsel (OGC). 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. For more information, see 29 CFR 1410.3, Individual access requests.

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

Requests for correction or amendment of records may be submitted to the Chief Privacy Officer at privacy@fmcs.gov or Chief Privacy Officer at FMCS 250 E Street, SW, Washington, DC 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 Shared Neutrals SORN and the Shared Neutrals 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

Describe risks currently related to the Department's access, redress, and correction policies and procedures for the system and what, if any, steps have been taken to mitigate those risks.

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 Shared Neutrals SORN and the Shared Neutrals SORN.

Section 8. Technical Access and Security

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

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

Management must approve any users accessing the system, and they submit a request to IT (SharePoint administrator) to have that user added to the Shared Neutrals SharePoint site.

8.2 Will FMCS contractors have access to the system and the PII? If yes, what involvement will contractors have with the 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?

FMCS contractors working on the SharePoint portal have some level of access to the Shared Neutrals site and the data within. However, these contractors are not working on the system specifically and therefore would not be

accessing it on a normal basis. Any contractors with access to FMCS systems must have completed an NDA with FMCS and have been through a background investigation and be cleared to access FMCS 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?

If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

This system is covered under the A&A issued to Microsoft for use of their desktop and cloud products.