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 the system to cover the Executive Branch Confidential Financial Disclosure Reports, and agency ethics guidance to employees and FMCS clients.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

In accordance with ethics laws, regulations, and the Code of Professional Conduct for Labor Mediators, FMCS will collect, store, evaluate, and disclose, when necessary, information pertaining to ethics and mediators. FMCS may disclose information pertaining to FMCS parties or clients to address impartiality concerns or explain mediator reassignments. Pursuant to the Code of Professional Conduct and FMCS's mission, the FMCS ethics system may include additional documents pertaining to mediator assets and client notices concerning those assets. This system of records supplements the Office of Government Ethics GOVT-2 system. This system will collect information from FMCS employees serving as mediators and federal employees serving in mediators' supervisory chain. In evaluating ethics concerns, FMCS may also gather information from internal agency sources and departments and store information as part of this system.

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?

These records contain statements and amended statements of personal and family holdings and other interests in property, income, gifts, reimbursements, liabilities, agreements, arrangements, outside positions, retirement products, pensions, and other information related to conflict-of-interest determinations. These statements include completed copies of the Office of Government Ethics (OGE) Form 450 and alternative confidential disclosure forms reflecting more detailed information pertaining to mediator pensions and supplemental agency ethics documents including, but not limited to cautionary memos, recusals, firewalls, waivers, authorizations, acknowledgment of duty to contact the Office of General Counsel, and any statements or certifications concerning no conflicts of interest.

Yes, the types of information collected, used, maintained, and shared are specified in its Privacy Notices.

PII Mapping Components

FMCS Ethics Records consists of FMCS-0006 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 Ethics 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
Office of General Counsel (OGC)	Yes	Names and information related to assets, outside positions, and etc.	reflects mediator obligations under the Code of Professional Conduct for Labor Mediators as referenced in 29 C.F.R. 1400.735-20; supplements the Office of Government Ethics GOVT-2 system; and meets the requirements of Executive Order 12674, as modified, 5 CFR part 2634, and subsequent agency regulations, as well as section 107 of the Ethics in Government Act of 1978, as amended.	Records are located in a locked file storage area or stored electronically in locations requiring agency network access via multifactor authentication. FMCS buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

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

Information in this system of records is provided by: 1. The Federal employee or a designated person such as a trustee, accountant, banker or relative. 2. Federal officials who review the statements to make conflict-of-interest determinations. 3. Persons alleging conflicts of interest or other violations of ethics laws and persons contacted during any investigation of the allegations. 4. FMCS clients, in accordance with 5 C.F.R. 2635.502 and the Code of Professional Conduct for Labor Mediators, acknowledging notice of impartiality concerns.

1.3 How is the information collected?

Information is collected from the source using email and Microsoft PowerApps.

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

This purpose is to reflect mediator obligations under the Code of Professional Conduct for Labor Mediators as referenced in 29 C.F.R. 1400.735-20. This system of records supplements the Office of Government Ethics GOVT-2 system and may contain records collected and maintained to meet the requirements of Executive Order 12674, as modified, 5 CFR part 2634, and subsequent agency regulations, as well as section 107 of the Ethics in Government Act of 1978, as amended. This system includes the additional collection, documentation, and disclosure of mediator ethical concerns regarding financial conflicts of interest and impartiality, including but not limited to, ethics waivers and authorizations.

1.5 How will this information be checked for accuracy?

Information is collected from the source.

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

29 U.S.C. 172, et seq. as it pertains to providing mediation and conflict resolution services to clients; Ethics in Government Act of 1978, 5 U.S.C. app. 101, et seq.; E.O. 12674 (as modified by E.O. 12731); 5 C.F.R. part 2634; 5 C.F.R. part 2635; and 29 C.F.R. part 1400.735-20.

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: These 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 Ethics System that will cover the Executive Branch Confidential Financial Disclosure Reports, and agency ethics guidance to employees and FMCS

clients 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

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.

This system is used to evaluate ethics concerns and provide ethics guidance.

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

A variety of reports are created in Microsoft Excel (or other analytics program such as Microsoft Power BI) to be filtered and analyzed as needed.

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 Ethics records are stored on FMCS shared drives and Microsoft 365 platforms, and the access are 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, requests for access go through the General Counsel's office.

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? The Office of Information Technology is responsible for assuring safeguards and management of the electronically 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 than 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

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?

Records are maintained for six years after filing, except when filed by or with respect to a nominee and the nominee ceases to be under consideration for the position. If any records are needed in an ongoing investigation, they will be retained for the duration of the investigation.

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 Employee Ethics Records, GRS 2.8, 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 multifactor authentication 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. Ethics records should be disposed of in accordance with GRS 2.8 issued by NARA.

Principle of Data Quality and Integrity: Ethics 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 with the employee's Supervisor in the PowerApp only to view and ensure spouse and dependent information is included on forms. After the Supervisor signs and sends the form back to the filer in the App, the Supervisor no longer has access to the information. Also, Cautionary Memoranda are shared with Supervisors in an email.

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?

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). Please see the routine uses section in the SORN for the information that is shared and the purpose.

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.

The sharing of information outside of the agency 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.

It is shared through protected links and email.

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**
Pursuant to the Privacy Act, all or a portion of the ethics records or information may be disclosed to authorized entities, as is determined to be relevant and necessary.	See the SORN routine uses.	See Section 1.1.	See Section 1.6 and the SORN routine uses for additional information.	Shared through protected links and email. Emails are secured in Exchange Online using Microsoft Government Community Cloud (GCC) processes.
The Office of Government Ethics as part of a program	Part of a program review, audit, or inspection	Financial disclosure forms and related documents	5 CFR 2638.400	Shared through protected links and/or email. Emails are secured in

review, audit, or inspection.				Exchange Online using Microsoft Government Community Cloud (GCC) processes.
The Office of Special Counsel in connection with an administrative proceeding.	Administrative proceeding or investigation	Financial disclosure forms and related documents	28 C.F.R. 600.4	Shared through protected links and/or email. Emails are secured in Exchange Online using Microsoft Government Community Cloud (GCC) processes.
The Department of Justice in connection with an administrative proceeding or other legal or enforcement action.	Administrative proceeding, investigation, or other legal or enforcement action.	Financial disclosure forms and related documents	18 U.S.C. 208	Shared through protected links and/or email. 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 Ethics 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 Ethics 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 is a Privacy Act Statement on the Ethics Form, and a system of records notice was published in the *Federal Register*. The system of records notice for the Ethics SORN is here and the Privacy Act Statement is here on the OGE's website on the Form.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is there a penalty?

Pursuant to 5 U.S.C. § 13109, Executive Order 12674 (as modified by Executive Order 12731), and 5 CFR Part 2634, Subpart I, of the Office of Government Ethics (OGE) regulations, the information on the form is required. Failure to provide the requested information may result in separation or disciplinary action.

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

The primary use of the information is for review by the Agency's Ethics Office to determine compliance with applicable Federal conflict of interest laws and regulations. Additional disclosures may be made pursuant to the SORN routine uses section.

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: FMCS provides notice to individuals regarding its collection, use, and maintenance of PII.

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

Risk Assessment: FMCS will evaluate the risk of a data breach in safeguarding personal information.

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 failure to provide the information. This risk is also mitigated since the notice of the collection of information is provided in the PIA available on the public facing website, the Privacy Act Statement on the Ethics Form, and by the notice in the *Federal Register* for the Ethics 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. See 29 C.F.R. 1410.3, Individual access requests.

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

Records are updated on a periodic basis; most record corrections can be handled through established administrative procedures. Contact the Office of General Counsel (OGC) for contesting records under the provisions of the Privacy Act. See 29 CFR 1410.6, Requests for correction or amendment of records, on how to contest the content of any records.

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

The PIA and the notice on the *Federal Register* 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: FMCS will evaluate the risk of a data breach in safeguarding personal information.

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

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?

Users request access to the system and the Office of the General Counsel (OGC) determines who needs access to the system servers, and in turn sends a request to the Office of Information Technology that access be provided to the user. Any users with administrative access to the system or servers must have valid FMCS credentials to log in to the system and use multifactor authentication for logins.

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?

Yes, some contractors will have access to the system. All contractors with access must have an NDA in place and a public trust background check completed.

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.

General FMCS systems including Microsoft 365 (SharePoint, Teams, OneDrive, PowerApps) and Microsoft Azure have A&A's in place to reflect FedRAMP moderate compliance.