FMCS | FEDERAL MEDIATION & CONCILIATION SERVICE

OFFICE OF GENERAL COUNSEL
PRIVACY IMPACT ASSESSMENT (PIA)

The completion of FMCS PIAs is mandated for any rulemaking, program, system, or practice that collects or uses Personally Identifiable Information (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

Section 208 of the E-Government Act of 2002 establishes guidance that government agencies protect and conduct privacy impact assessments (PIA) on how data is collected, store, and shared from electronic systems. It's important how this information will be disseminated and maintained.

The Privacy Act of 1974 states how government agencies should protect records about individuals and their information that governs the collections of personally identifiable information that is maintained in systems of records by federal agencies. It ensures that we follow applicable laws and regulations to prevents risk to shared information and how this information is being used.

Overview

Federal Mediation and Conciliation (FMCS) uses Collabspace to manage electronic data such as electronic records and electronic emails. Collabspace is an Electronic Records Management (ERM) system that is used to manage all phases of electronic records across a unified platform hosted in a cloud repository using Microsoft SharePoint, Exchange Online, File Share, SharePoint lists, and SharePoint Libraries.

The FMCS Records Officer uses Collabspace to collect data from individual departments to manage records life cycles until the end of their destruction dates. Each Department have file plans with General Records Schedule information and the Agency Comprehensive Schedules. Collabspace securely stores all records within the system until a triggering event occurs, prompting their destruction with certification.

Event triggers are initiated by actions such as workflows based on a specific event or condition. For example, an event trigger can be set up to send email notifications to team members when a new document is added to a share folder, or a record has reached its retention date based on the last modified or creation date. Event triggers can be extremely helpful for automated repetitive task.

Section 1. Characterization of the Information

The FMCS Records Officer collects file plans from each Department so they can be integrated into Collabspace, and retention policies and workflows are applied. There are security groups as part of the review process when it's time for records destruction. The system is developed based on a cloud-based infrastructure using Microsoft 365, SharePoint, and File Shares.

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 Agency's file plans including FMCS' Comprehensive Records Schedules and the General Records Schedule (GRS) are collected, used, and maintained in our Electronic Records Management System. Collabspace collects user profile information such as email addresses and user role details. The system also collects information content such as files and images along with meta data. This information is shared between the

National Archives Records Administration (NARA) and FMCS. All data in the system is protected, secured, encrypted with WORM-compliant storage with Microsoft Azure, and in line with the Privacy Act regulations.

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

PII Mapping Components

Collabspace consists of FMCS-0013 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Collabspace and the functions that collect it are mapped below.

The collection of PII originates from Department records. Collabspace retains the documents and history within the Departments. Notification for the collection has been completed within that Department.

PII Mapped to Components				
Components	**Does this function collect or store PII? (Yes/No)**	**Type of PII**	**Reason for Collection of PII**	**Safeguards**
Agency Departments	Yes	Email addresses, addresses, phone numbers, and names	collect, create, and maintain FMCS records through its records life cycle	System is housed in a secure, FedRAMP-authorized cloud location. Only personnel authorized with a need-to-know are authorized to access the system.

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

The sources of information in the system are from each Department within the Agency. Source locations are Exchange Online, File Shares, and SharePoint including document libraries and lists.

1.3 How is the information collected?

File Plans are collected from every Department via email and ingested into Collabspace, the Agency's Records Management System. The information is needed to apply retention policies in line with NARA's laws and regulations. Email is managed based on NARA's capstone approach, GRS 6.1.

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

The purpose of this information is to use Collabspace as a vehicle to collect, create, and maintain FMCS

records through its records life cycle. The Federal Records Act, 44 U.S.C. § 3101, requires all Federal agencies to make and preserve records containing adequate and proper documentation of organization, functions, policies, decisions, procedures, and essential transactions. Collabspace is a Records Management and Retention system for managing records produced by FMCS.

The system manages Agency emails in accordance with GRS 6.1 for agencies that implement the Capstone Approach. Capstone officials are permanent and non-capstone accounts have a seven-year retention schedule.

1.5 How will this information be checked for accuracy?

Records in the Federal Government are subject to various checks and balances to ensure accuracy, compliance, and the reliability of agency records. The Agency's Records Officer checks the accuracy of the records added to Collabspace. Each agency is assigned an Appraisal Archivist at NARA who is responsible for ensuring the accuracy of agency records and compliance. The Appraisal Archivist collaborates with the Agency's Records Officer and NARA. They play a significant role in the value, preservation, memory, historical value, safeguards, and the accuracy of an agency's federal records. NARA is checking to ensure the correct retention schedule is applied to each record.

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

The collection of information for records management are governed by various legal authorities listed below:

Records Management by the Archivist of the United States by the Administrator of the General Services, 44 U.S.C. 29; and
Records Management by Federal Agencies, 44 U.S.C. 31 et seq.

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: To define records retention policies that are governed by NARAs policies, laws, and regulations.

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

Principle of Individual Participation: All data in the system is protected and encrypted. Only those personnel with proper permissions can perform an elevated discovery search. Collabspace can perform an elevated discovery search for an individual and a review of destruction of records when requested.

Principle of Data Quality and Integrity: FMCS system administrators ensures that the data/information collected is encrypted, WORM- compliant and stored within the Collabspace cloud. The data is not modified or shared with unauthorized users. The Agency Records Officer verifies the records are accurate and the Records Liaisons for the Departments verifies the locations of the records.

Risk Assessment: Low Moderate.

Privacy Risk: Low. The system will only use data that is collected for the purposes it is intended for.

Mitigation: Collabspace has many security standards mitigating risk. Collabspace is a permission-based system, and only authorized users have access to it and its contents. Some of the standards includes requiring authentication to access data and setting user permissions and privileges with logging enabled. Data is encrypted with security and compliance awareness. Collabspace leverages Microsoft Azure securing source code and system updates. Collabspace captures multi-repository content and all version changes. Using encrypting methods for data in transit and at rest with storing data in multiple data centers. Collabspace has advanced protection from Ransomware with WORM-storage, detecting potential vulnerabilities and backup in case of disaster. The Collabspace team stays updated on current/latest information security policies and training.

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 information in the system will be used to manage FMCS electronic records and email in support of our records management program to support the mission of our Agency.

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

The data in the system is analyzed using cloud base functionality via all SharePoint files including lists and doc view files, File Sharing and Microsoft 365 email. Data is not being produced, but a retention policy is being applied to the data.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII? **(Answer all questions)**

How is access to the PII determined? Access is determined by the Records Manager, Departments, and Technical Administrator. Therefore, only authorized personnel needing access are allowed to use the system.

Are criteria, procedures, controls, and responsibilities regarding access documented? Yes, criteria, procedures, controls, and responsibilities regarding access have documented permissions and a recorded log of access.

Does access require manager approval? Access in Collabspace is generated on permissions that is set by the administrators or owner of the system. Generally, access to the system is governed by users or members with a particular access to include a System Administrator, User Administrator, Records Administrator user role, Search Administrator, Physical Records Administrators, Global Administrator, Discovery Administrator, and basic user. Each permission is only allowed access to perform duties within a user permission.

Is access to the PII being monitored, tracked, or recorded? Yes, access to Collabspace has safeguards, including requiring authentication to access data, setting user permissions and privileges with logging/ tracking enabled.

Who is responsible for assuring safeguards for the PII? Within Collabspace, the Collabspace Administrator in conjunction with Collabware are responsible for assuring safeguards for the PII. In addition, the IT Department and the IT Administrator of the system are responsible for ensuring that the network locations (either on premises or in the cloud) are secure, and meeting access and security requirements set by CISA (Cybersecurity and Infrastructure Security Agency).

Principle of Transparency: FMCS is transparent in the use of individual data as stated or described in the SORN.

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

Risk Assessment: Low Moderate.

Privacy Risk: The privacy risk in Collabspace is low. Typically, permissions are determined by the administrator and its risk against potential exposure of sensitive information or unauthorized users. To alleviate the potential risk, the system has functionalities that implement strong access controls and permissions, and the Agency educates users on best practices and monitors users' activities to prevent unauthorized access.

Mitigation: Collabspace has many security standards mitigating risk. Collabspace is a permission-based system, and only authorized users have access to it and its contents. Some of the standards includes requiring authentication to access data, and setting user permissions and privileges with logging enabled. Data is encrypted with security and compliance awareness. Collabspace leverages Microsoft Azure securing source code and system updates. Collabspace captures multi-repository content and all version changes. Using encrypting methods for data in transit and at rest with storing data in multiple data centers. Collabspace has advanced protection from Ransomware with WORM-storage, detecting potential vulnerabilities and backup in case of disaster. The Collabspace team stays updated on current/latest information security policies and training.

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?

All FMCS electronics records and emails will be retained until they are dispositioned.

3.2 How long is information retained?

All records are retained and disposed of based on the retention polices governed by NARA. See Disposal of Records, 44 U.S.C. 33. This would include the General Records Schedules and Agency Comprehensive Schedules.

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 General Records Schedules have been approved by NARA; the Agency Comprehensive Schedule is pending approval by NARA since the Agency has gone through several re-alignments. The Agency wants to ensure those records are updated with the correct schedules. Therefore, the pre-approval process is necessary to update the Agency's schedule.

The names of the records retention schedules are as follows:

Finance, GRS 1.0
Human Resources, GRS 2.0
Technology, GRS 3.0
Information Management, GRS 4.0
General Operational Support, GRS 5.0
Mission Support, GRS 6.0

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; and (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?

PII is not used for research, testing or training because this is a records system, all training and testing is done with low risk (non-PII) and/or dummy data.

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: FMCS only collects PII that is directly relevant and necessary to accomplish the specified purposes and only retains PII for as long as necessary to fulfill the specified purposes. PII should be disposed of in accordance with the Agency's Comprehensive Records Schedules as approved by NARA and NARA's General Records Schedules.

Principle of Data Quality and Integrity: FMCS ensures that PII is accurate, relevant, timely, and complete within the context of each use of the records. Pursuant to 44 U.S.C. 31, Records Management by Federal Agencies, file plans are reviewed by the Agency's Records Officer to ensure that they comply with the law and regulations by NARA.

Risk Assessment: Low Moderate.

Privacy Risk: The Privacy Risk is retaining too much information past the retention policy.

Mitigation: Content/data is retained only as long as required by the records retention schedules and in conjunction with NARA requirements. Content/data is disposed of within Collabspace.

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/received? What information is shared/received, and for what purpose? How is the information transmitted or disclosed?

Records information may be shared with the owners of that content when they have a need-to-know. In addition, information may be shared with the Office of Human Resources and the Office of the General Counsel when proper authority is given for issues such as litigation or discovery.

The information FMCS shares or receives is listed in Section 1.1. Each Department will have their files setup with a retention policy based on locations of their files and this will feed into Collabspace.

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.

To share information from the records system, proper authorization must be obtained by the recipient. There is a risk that once the information leaves the records system it is improperly shared with others. However, aside from the assurance given by the recipient, there is little FMCS can do to mitigate the issue. That said, the risk for the improper sharing of data within FMCS is low.

Risk Assessment: Low.

Privacy Risk: Low. There is a risk that once the information leaves the records system it is improperly shared with others.

Mitigation: Steps are taken to confirm that the information being released is authorized and needed. These steps include written authorization signed by a management approved official and written confirmation that the data will be used for only those purposes for which it is authorized.

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/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?

Information will be shared with NARA once records reach the end of their life cycle.

All information will be transmitted electronically in accordance with safeguards of records. 44 U.S.C. 3103.

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).

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.

Information is transmitted to external entities using SFT site that is encrypted. A password link is provided in a separate email when a link is requested to ensure that the information being sent is protected and secure.

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
NARA	Adhering to the NARA's policies, laws and regulations.	Agency Comprehensive Records Schedules	44 U.S.C. 31; and the 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).	NARA sends an encrypted direct link to upload records.

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: Information is only shared with NARA unless otherwise specified in the SORN routine uses section.

Privacy Risk: Low. Information is being sent with an encrypted link.

Mitigation: Information is shared only with NARA when necessary to adhere to records retention requirements. All data is transmitted to NARA using secure, encrypted protocols. Data is encrypted with security and compliance awareness. Collabspace leverages Microsoft Azure securing source code and system updates. Using encrypting methods for data in transit and at rest with storing data in multiple data centers. Collabspace has advanced protection from Ransomware with WORM-storage, detecting potential vulnerabilities and backup in case of disaster.

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, a system of records notice is published in the *Federal Register* 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 maintain agency records.

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

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, dissemination, and maintenance of PII. PII must be described in the Collabspace SORN.

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

Risk Assessment: Low.

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 notice of the collection of information is provided through the PIA available on the public facing website, and the systems of records notice in the *Federal Register* for the Collabspace 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 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?

Collabspace does not determine the accuracy of the information beyond file plans and the Records Policy. File plans and the Policy can be corrected with coordination and collaboration of the Agency's Records Officer or Records Liaison Officers within Departments.

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?

This PIA for Collabspace and the Collabspace 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: The individual already consented to the original Department's request. Collabspace retains that information until the specific retention policy.

Risk Assessment: Moderate-Low.

Privacy Risk: Within Collabspace, Low/Moderate. 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 Register* so individuals are aware of the process for accessing and/or correcting information. Collabspace is a permission-based system and only authorized users have access to it and its contents. Collabspace has advanced protection from Ransomware with WORM-storage, detecting potential vulnerabilities and backup in case of disaster.

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?

Policies have been written which outline who can access Collabspace and for what reasons. The system is role based, with least-privileged access roles assigned. Currently, only Records Administrators and technical support have access to the administration of the hosted system. Only FMCS Collabspace technical personnel have access to the servers that house the agent and adapters used by Collabspace.

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, Collabspace is developed in conjunction with contractors. Contractors provide valuable designs and insights into the development of the system. NDAs are required of all contractors and any contractor accessing FMCS data must pass a Tier 2 Public Trust clearance.

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

Collabware University is available to users of the system and provides all needed skills to manage and administer the 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.

Yes. The ATO was granted on February 20, 2024, and filed with FedRAMP.