FMCDB Privacy Impact Assessment Addendum

Reason: Temporary Database Relocation to Azure

This addendum supplements the existing FMCDB Privacy Impact Assessment and documents the temporary relocation of the FMCDB database to FMC's authorized Microsoft Azure environment.

Unless expressly supplemented below, the original PIA remains unchanged.

Section D.1: If the system is hosted and/or used at more than one site, how will consistent use of the system and data be maintained at all sites?

The FMCDB database, previously hosted on an on-premises SQL Server, is being temporarily relocated to a SQL Server virtual machine within FMC's existing authorized Microsoft Azure environment.

The internal and external-facing web servers will remain within FMC's on-premises infrastructure.

The application will continue to access the same underlying database through agency-approved network connectivity. The relocation does not change the intended collection, maintenance, processing, or use of information.

The FMCDB system will retain its existing authorization boundary and leverage applicable security controls from FMC's authorized Azure hosting environment.

Section D.4: Is the system using technologies in ways that the FMC has not previously employed (for example, monitoring software, CallerID)? If yes, how does the use of this technology affect public/employee privacy?

Yes. The system is being temporarily hosted using Microsoft Azure infrastructure already authorized for agency application and database hosting.

The change introduces cloud-based database hosting but does not introduce new application functionality, methods of information collection, or intended uses of personal information.

Privacy risks associated with the relocation, including administrative access, network connectivity, data storage, and backup handling, will be addressed through applicable agency security controls.

Section D.7: If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The existing FMC-41 System of Records Notice remains (SORN) applicable. The temporary relocation of the FMCDB database from an on-premises SQL Server to a Microsoft Azure cloud environment does not constitute a significant change that is substantive in nature to warrant modifying the existing FMC-41 SORN. For example, the infrastructure relocation does not change the categories of records, categories of individuals, purposes, or intended routine uses described in the existing FMC-41 SORN. Also, as described in Section E.1 below, the infrastructure relocation will inherit the existing access control.

Section E.1: Who will have access to the data in the system (for example, contractors, users, managers, system administrators, developers, other)?

Existing application-level access permissions and user roles will remain unchanged.

Database and infrastructure administrative access will be managed through FMC's established access-control procedures and applicable Azure security controls.

The relocation does not authorize additional access to personal information or expand the categories of individuals permitted to access FMCDB records.

Appendix II, Question 3: What impact will this system have on an individual's privacy? (Consider the consequences of collection and flow of information and identify and evaluate threats to individual privacy.)

The primary privacy implications of this modification relate to relocating database storage and administrative operations from on-premises infrastructure to Azure.

Potential risks include unauthorized administrative access, exposure through network connectivity, and improper handling of database backups.

These risks will be addressed through existing and applicable FMC security controls, including access restrictions, encryption, network security, monitoring, and backup protections.

The relevant controls will be validated through the system restoration security assessment.

Appendix II, Question 4: As a result of the PIA, what choices have been made regarding the IT system of collection of information? Have adequate measures been designed and implemented to mitigate risk? What is the rationale for the final design choice or business process?

The temporary relocation was selected in response to an unforeseen infrastructure failure affecting FMC operations.

The existing Azure environment is authorized to host agency application databases on virtual machines.

The relocation enables restoration of existing FMCDB services without introducing new application functionality or changing the intended collection and use of personal information.

The system will remain subject to FMC's established security authorization and risk management processes.

Approval of Privacy Impact Assessment accuracy and completeness.

System Owner: [redacted] Digitally signed by MOHAMMAD USMAN Date: 2026.10.29 12:21:35 -04'00'

Signature Date

Business Owner:

Signature Date

Approval of IT System Risk Assessment

Chief Information Officer: [redacted] Digitally signed by MOHAMMAD USMAN Date: 2026.10.29 12:22:01 -04'00'

Signature Date

Approval of Privacy Assessment and Resulting System Categorization

Senior Agency Official for Privacy: [redacted] Digitally signed by CINDY HENNIGAN Date: 2026.10.29 12:34:48 -04'00'

Signature Date