United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Microsoft 365 (M365)		**System Owner:** Fisseha Kefle	
Preparer: Lawrence Lee		**Office:** OFA/OITO/ECSD	
Date: 03-19-2026		**Phone:** (202)-566-1042	
Reason for Submittal:			
New: ☐	Revised:☒	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☒	Rescindment/Decommission: ☐		

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

Microsoft 365 (M365), also known as My Workplace, is a component of Email and Collaboration Solutions (ECS), is a Microsoft Government Cloud Community (GCC) Multi-Tenant (MT) FedRAMP approved Software-as-a-Service (SaaS) computing-based subscription service. M365 is the Agency's communication and collaboration system used to enhance workplace productivity. Furthermore, in the last several years the system has evolved to include a variety of tools and services that have helped to increase both efficiency and communication within the agency. These suite services function as the Agency's official communication and collaboration system that includes the following applications/tools: Word, Excel, SharePoint, Teams, Exchange online, Power Platform, Power Pages, etc. Thus, making it easier for the Agency's multi-disciplinary, geographically dispersed workforce stays better informed by facilitating

communication, coordination, collaboration, and innovation allowing EPA to deliver better on its mission of protecting human health and the environment. M365 uses personalized profiles for each EPA employee or contractor in the EPA Agency directory. These profiles include the following datatypes: work-related information (office location, office phone number) as well as optional information voluntarily provided by the employee such as work experience, educational history, and may include photographs.

In addition, the M365 suite includes data types that are uploaded by the EPA M365 user community (i.e., EPA employees/contractors) and are maintained in applications like SharePoint, Email, Power Platform, and OneDrive. The infrastructure supporting these applications will be managed by the M365 team, however the responsibility for controlling access to data uploaded is the responsibility of the site owner. The storage of these data types is being included in M365 to provide further collaboration and for the purpose of fulfilling the EPA's mission. A complete list of these data types has been provided in section 2.1.

Section 1. Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

- 5 U.S.C. 301 "Departmental Regulations". The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.

- 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014. Codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies and assisting OMB in developing those policies.

- Information Technology Management Reform Act (Clinger-Cohen Act). Public Law 104-106, 1996. – Provides the Agency's CIO responsibility for "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency" (Sec. 5125(b)(2)) and "promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency" (Sec. 5125(b)(3)).

- 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.

- OMB Circular No. A-130 – Management of Federal Information Resources. The Circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. The Circular promotes innovation, enables appropriate information sharing, and fosters the wide-scale and rapid adoption of new technologies while strengthening protections for security and privacy.

- Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011. Requires agencies that provide significant services directly to the public to identify and survey their customers, establish service standards and track performance against those standards, and benchmark customer service.

- Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011. Gives FedRAMP the authority to provide a cost-effective, risk-based approach for the adoption and use of cloud services for Executive departments and agencies.

.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

M365, a component under Email and Collaboration Solutions (ECS), has a completed System Security Plan (SSP) with an ATO that expires on October 31, 2026.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FEDRAMP approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, the system is cloud-based in which data will be maintained and stored. The Cloud Service Provider (CSP) is FedRAMP approved. M365 is a SaaS cloud platform.

Section 2. Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

A small portion of the data M365 collects and maintains is from Active Directory, such as username and LanID. Other data fields collected include employee names, username, work email address, work phone number, work address, title of EPA employee and contractor, and related organizational information required for system administration. Data Loss Prevention does not collect the aforementioned datatypes; however, it is used more for blocking information from leaving the agency for these datatypes.

These identifiers are collected and maintained for authentication, access management, collaboration, and communication within the Microsoft 365 environment. While users may

search for colleagues by name, email address, or username to facilitate communication and document sharing, this functionality is incidental to collaboration and does not constitute retrieval of a Privacy Act 'record' about an individual. The system is not designed to retrieve information about individuals by personal identifier for the purpose of creating or maintaining a Privacy Act system of records. This table shows the datatypes that are tagged for use with DLP:

Data Elements in M365 (Including Email, SharePoint, Power Platform OneDrive, etc.)			
Field Label	**PII**	**SPII**	**PHI**
Username	X	No	No
Employee Names	X	No	No
Work Email Address	X	No	No
Work Phone Number	X	No	No
Work Address	X	No	No
Title Of EPA Employee and Contractor	X	No	No
Related Organizational Information Required for System Administration	X	No	No
Personal Email Address	X	No	No
Personal Phone Number	X	No	No
Office Name	X	No	No
Mail Code Address	X	No	No
Occupational Series	X	No	No
Pay Grade	X	No	No
Bargaining Unit	X	No	No
Accommodation Requested	No	No	No
Accommodation Request Date	No	No	No
Accommodation Determination Date	No	No	No
Field Label	**PII**	**SPII**	**PHI**

Data Elements in M365 (Including Email, SharePoint, Power Platform OneDrive, etc.)			
Accommodation Determination Method	No	No	No
Explanation Of Method	No	No	No
Status	No	No	No
Decision-Making Official Name and Title	X	No	No
Disability Status	X	No	No
Medical Information Request Tracking Data	No	No	X
Disability Determination Tracking and Status	No	No	No
Medical Information Recipient Name	X	No	No
Medical Information Release Form and Related Tracking Data	No	No	No
Reconsideration Tracking Data	No	No	No
Data Concerning Communication of Decisions	No	No	No
Accommodation Offer Notification and Related Comments	No	No	No
Medical Documentation (If provided)	X	X	No
Field Label	**PII**	**SPII**	**PHI**
Confirmation of Request for Reasonable Accommodation Form	No	No	No
Denial of	No	No	No

Data Elements in M365 (Including Email, SharePoint, Power Platform OneDrive, etc.)			
Reasonable Accommodation Request Form			
Reasonable Accommodation Information Reporting Form	No	No	No
Checklist for Obtaining Medical information	No	No	No
Reasonable Accommodation (if needed)	No	No	No
COVID Vaccination Status Exceptions (Including Religious Data) Considered medical information	No	X	No
US Individual Taxpayer ID Number	X	No	X
US Social Security Number	No	X	No
US / UK Passport Number	No	No	No
ABA Routing Number (Financial)	No	X	No
Credit Card Number (Financial)	No	X	No
Field Label	**PII**	**SPII**	**PHI**
US Bank Account Number (Financial)	No	X	No
US Driver's License	No	X	No

2.2 What are the sources of the information and how is the information collected for the system?

Microsoft 365 receives core user identity information from Active Directory, including username, user principal name (PN), work email address, office location, office phone number, and organizational attributes. This information is synchronized to M365 to enable authentication, access management, licensing, and collaboration features. Employees may also

voluntarily provide optional profile information such as photographs.

Additional information within the M365 environment is generated by users through normal business activities, including email, Teams communications, SharePoint sites, Power Platform applications, and OneDrive files. This content is created and maintained by users and stored within the respective M365 services; it is not collected by M365 for the purpose of retrieving records about individuals.

System-generated metadata (timestamps, audit logs, file ownership, and access history) is created automatically to support security, compliance, and operational functionality. Privileged administrators manage this information solely to support system operations and data governance.

.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, M365 does NOT use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the data is ensured by several components and tools that work to provide web filtering, data accuracy, Data Loss Prevention (DLP), monitoring tools, and Advanced Information Protection (AIP). Also, it is the responsibility of the system owner and each licensed user to ensure accuracy of data at the time the data is created or used within email and SharePoint. Additionally, there are CUI marking tools and other Microsoft components for documentation tracking that provide data accuracy mechanisms.

The specific tools used for ensuring the data include (1) Data Loss Prevention (DLP) and (2) the Microsoft Purview engine (previously Compliance Center). The Microsoft Purview engine uses a feature called Content Explorer that shows all detected Sensitive Information Types (SITs). This allows the administrator/s to drill down to see the actual locations, users, and content. Also, the M365 Data Loss Prevention (DLP) tool uses the same SITs detection engine and is currently in use within the EPA to filter out sensitive datatypes not specifically pre-approved by EPA/administrators.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included

Privacy Risk:

There is an inherent risk to the privacy of individuals for the use of M365 due to the nature of the information being shared which includes PII. This level of risk associated with the type of PII is dependent on the office or program use and the safeguards implemented to mitigate the risk. Information stored within Microsoft Teams includes name, email address, work phone, work address, and title of EPA employees and contractors. The use of SharePoint Online and Power Platform allows some PII such as personal phone number, home phone number to be entered and stored in the system and may

include other personal information such as the employee personal contact information.

Mitigation:

M365 is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. M365 is rated as FISMA moderate based upon the type and sensitivity of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system.

The Service Level Agreement between EPA and Microsoft GCC M365 services does not allow the service provider to review or audit EPA data, which minimizes privacy risks from the vendor source. All EPA employees and contractors must complete privacy, security, and records management awareness training, as well as role-based training where applicable, on an annual basis. To help mitigate the privacy risks, EPA has some administrative, technical, and physical controls in place. M365 is only accessible by authorized licensed users. Prior to granting users access to the EPA network, all users must agree to the EPA Rules of Behavior, as well as the EPA Warning Banner before accessing the system, which includes the consent to monitoring, and restrictions on data usage. EPA's user identity management processes include password hash syncing which helps to enforce encryption mechanisms to prevent unauthorized use of M365. System administrators manage access through ACLs and group policies.

As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the M365 environment, which will help the agency effectively maintain our privacy and security posture for the system. The system security plan is reviewed annually to ensure adequacy of controls implemented to protect data.

Section 3. Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

Yes, M365 user accounts are managed using Privileged Access Management and Role Based Access Control (Conditional Access Rules) that can be defined by the administrative user. Access can be revoked or edited by the site owner using Access Control Lists (ACL). Users authenticate through using Multifactor Authentication (MFA) and the Privileged Identity Management (PIM) to gain access to M365. Attempts at unauthorized access are captured and reported by the NetPro tool suite.

The system also includes restrictions on computer access to authorized individuals only, required use of strong passwords that are frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals only, and by maintaining records in lockable offices and filing cabinets.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

There are several policies and procedures that are managed by several different groups within the EPA. These documents include but are not limited to the following: EIAM SSP, M365 Account Management Procedure Guide, ProMicrosoft Online NetPro Users Guide, DLP Content Explorer Guides, etc.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. There are no other components with assigned roles and responsibilities within M365.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Both Government and contractor employees have access to the data/information in M365. Data access must be EPA approved by EPA partners/federate organizations to have access to the data and information contained within the system.

Additionally, all EPA personnel and approved partners/federation groups/individuals must have proper multi-authentication credentials to be able to access the data in M365.

The appropriate FAR clauses, CFR 24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act, have been incorporated into the contract and provide a foundation for the contractor's privacy data protection policies.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

M365 follows Records Control Schedule 1006 and 0759. All information is retained in the cloud for a period of a year after there is no contract/service. For standard EPA users, Capstone policy sets email retention at 10 years. For exempted EPA users such as employees under a Litigation Hold, Super Fund Hold, Enforcement Hold, and Capstone Officials, emails are kept indefinitely or until the hold is removed.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system

Privacy Risk:

The length of time is per Capstone, however; there is a low risk of incidents involving emails accidentally deleted before their date of expiration which could impact investigations.

Mitigation:

To mitigate this risk, M365 information (email, documents, chat logs) are backed up across at least two data centers in the Cloud. This allows records to be recalled for any after the fact investigations or queries through a ticket requested from ServiceNow.

Section 4. Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes, M365 shares information outside of EPA, however, it only shares information with authorized external entities and partners of the EPA. These types of external partners include business partners, third party security assessors, or those who have express authority on behalf of the EPA. Information is shared and accessed through the EPA intranet for collaboration purposes and for identifying the appropriate individuals (with appropriate licenses) for accessing email, SharePoint, PowerPoint, and other M365 services/applications.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The original purpose of M365 is to be used by EPA employees, authorized contractors, and authorized external partners as a platform for communicating and sharing information.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

ECS ISA/MOU Process: The ISA/MOU is first drafted and sent over to OFA SIO and ISO to review for accuracy and compliance. OFA ISO then reviews for any potential security risk. Next, EPA OFA OITO/EHD reviews for compliance and validates connections and will respond with EHD concurrence. It then goes back to the SIO for review and records. This same document that was sent to the SIO also goes back to the ISO for final review. The SIO receives the final reviewed document from the ISO. The SIO then validates the ISA/MOU with their signature and ISO then validates it with their signature. The final approved and signed document is then added into Xacta.

Currently there are no ISA/MOUs with any internal or external organizations.

4.4 Does the agreement place limitations on re-dissemination?

No, there are no limits on re-dissemination.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

There is a low risk in some private information such as phone number or name being used outside the agency, due to users recording or keeping shared information and/or emails with sensitive details. All M365 users sign a Rules of Behavior before access to the system is allowed and are expected only to

share information needed for their job roles/function. The information is not specifically relevant or purposeful to the intent of the sharing, i.e., no PII other than name and phone number is shared. This information is only integral to participation in the meeting/communication/email.

Mitigation:

EPA has initiated certain measures to ensure PII and information on individuals and sensitive data is not shared outside the agency by using Data Loss Prevention (DLP), which when implemented can limit and provide accountability for any information that is shared externally.

Section 5. Auditing and Accountability

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

5.1 How does the system ensure that the information is used as stated in Section 6.1?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The US EPA implements a Rules of Behavior (RoB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Information Security and Privacy Awareness Training (ISPAT) which is required annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There is a low risk that some M365 users may not complete required training on time according to the EPA's annual training policy.

Mitigation:

EPA's Privacy Awareness and Training Office will remove access to an individual if they do not complete the mandatory training required. This will disallow all users access to the application.

Section 6. Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

A small portion of the system information is collected and used for access/permissions that allow groups or individuals to use specific applications or features. Examples include rights to SharePoint folders, Power Platform, OneDrive, Exchange (administrators), or other tools for monitoring, such as Data Loss Prevention or administration of specific groups/Team's safe attachments/links and folders. Other groups within the EPA use SharePoint sites and Power Platform in order to share special or sensitive data for the purposes of collaboration and communication for operational projects or other EPA-related initiatives..

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: X No: ☐ If yes, what identifier(s) will be used.

A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.

M365 allows access to SharePoint, Power Platform and OneDrive as access dictates for specific folders that have been provided control/restrictions to by M365 administrators. Administrators or users can type in the Outlook address area a person's last/first name in order to email that user or to see information based on their access and retrieve information for that user by typing in the known name of the individual or email. Once that information comes up, it will provide a link to SharePoint and details about that individual being in the information system, so that they can be contacted.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

The EPA's security team is currently reviewing and updating the M365 Privacy controls to reflect the current state of M365 relevant to the privacy of individuals whose information is maintained in the system. Several tools mentioned in this PIA have been tested and implemented to protect the privacy of individuals within the system of records, such as DLP and certain content/filtering type mechanics and tools that help to ensure the effect of the privacy and data types housed within the system. These controls are tested and updated annually and include administrator and technical controls, as well as any vulnerabilities that may exist on a 72 hour-scan basis. All system security controls are tested annually as part of the 3PAO assessment, scheduled to be tested again in June of 2026. The system currently is under an ATO that expires on October 31, 2026.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is always a risk of misuse of information by both authorized and unauthorized users of M365.

Mitigation:

Data is restricted based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls. Access to customer data is also strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The M365 landing page has a Term of Use statement that the user must accept to continue to use the site. Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of the collection or sharing of their information?

Each user voluntarily provides minimum information and consents to Rules of Behavior before being granted access to EPA computer network and resources. Requesting access and using the services are voluntary; however, the employee information used is required to create and activate the user accounts to access these services. Not providing information prevents the user from accessing the EPA network and computing resources as EPA employees' username and contact information is provided by EPA employees for the essential purpose of user access control and account management within the EPA domain to complete their job duties in the course of conducting official business. Initial profile information in M365 will be populated using EPA's existing directory information; however, users will have the ability to update and manage their profiles. This collection and use of information is covered under System of Records Notice (SORN) EPA-64.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information.

Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

A low risk exists for users of ignoring any warning banners or use notices. There also may not be enough detailed information to educate the user in those banners/warnings through a lack of policy guidance.

Mitigation:

Warning banners & Terms of Use are provided which states information is not considered private and is subject to sharing and monitoring. This information can be used for the Freedom of Information Act as well. This information is provided for the system's intended purposes and is sufficient for M365.

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

The EPA provides login credentials to register with the EPA and access their individual Office 365 / My Workplace profiles through the EPA Web Portal/Virtual Private Network. EPA personnel also may contact the EPA help desk.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

Once individuals sign up for an account and are designated a password and user ID, they may validate their account. The EPA help desk may also assist with questions for any misinformation.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and Freedom of Information Act (FOIA).

Privacy Risk:

Little to no risk. M365 will leverage established EPA procedures for redress and follow SORN procedures.

Mitigation:

EPA will always provide access and amendment of M365 for individuals. EPA notifies individuals of the procedures for correcting their information in this PIA, Privacy Act Statement, through the EPA internal website (EPA personnel only) and through Microsoft and M365 administrators for any issues regarding redress.

I attest as the Agency Privacy Officer that the **Microsoft 365 (M365)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.05.20 16:18:15 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA