Privacy Impact Assessment for
OPM Artificial Intelligence (AI) Services

March 30, 2026

Contact Point

Benjamin McChesney
Supervisory IT Specialist
Office of Chief Information Officer / Enterprise
Information Systems/Network Management

Reviewing Official

Becky Ronayne
Senior Agency Official for Privacy

Abstract

OPM AI Services is a group of cloud-based artificial intelligence (AI) applications used to support productivity, content management, and communication. These services provide capabilities such as chat-based assistance, code generation, data analysis, and integration with enterprise applications including email, calendars, and external Application Programming Interfaces (API).

Overview

OPM AI Services consists of approved AI Software-as-a-Service (SaaS) applications that operate under the same privacy, security, and governance protocols. At the time of this assessment, approved applications include xAI Grok, Microsoft 365 Copilot, and OpenAI ChatGPT Enterprise.

These services use Large Language Models (LLMs) to generate and process text and may integrate with enterprise applications such as Outlook, Teams, SharePoint, Adobe Acrobat, and GitHub through secure connectors. These integrations allow authorized users to retrieve and process information within approved environments.

This Privacy Impact Assessment (PIA) applies to AI tools that operate under substantially similar functionality, data use, privacy controls, and security architecture. This includes tools that meet OPM's established criteria for internal use and approved deployment environments, as described in this assessment. Tools that introduce materially different capabilities, data uses, or privacy risks may require a separate PIA.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

OPM's use of AI tools is governed by the following authorities:

- EO 14179, *Removing Barriers to American Leadership in Artificial Intelligence* (January 23, 2025);
- EO 14319 *Preventing Woke AI in the Federal Government* (July 23, 2025);
- EO 14320, *Promoting the Export of the American AI Technology Stack* (July 23, 2025);
- OMB M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* (April 3, 2025);

- OMB M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (April 3, 2025);
- OMB M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (March 28, 2024).

OPM evaluates AI services for inclusion under this PIA based on shared characteristics, including but not limited to internal-use deployment, standardized security controls (e.g., identity management and multi-factor authentication), consistent data handling practices, and limited data retention periods. If future AI tools introduce materially different functionality, data uses, or privacy risks, OPM will update this PIA or conduct a separate PIA, as appropriate, and in accordance with applicable OMB guidance.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information in OPM AI Services is covered by OPM/Internal-3, Information Technology, Information System, and Network Activity and Access Records, as well as potentially by other OPM SORNs, depending on the subject matter of any output used for agency decision making.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

A Security and Privacy plan is currently in development.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, GRS 3.1 and 3.2 apply, as well as potentially other records schedules depending on the subject matter of information used and generated.

1.5. 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.

Not Applicable.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

AI services potentially use, collect, and disseminate information provided by authorized users through prompts, uploaded documents, or integrated enterprise applications.

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

Information may be provided by authorized OPM personnel in the course of performing official duties as well as through integrated enterprise applications. User provided information may include, but is not limited to, information from OPM systems, enterprise applications (e.g., Microsoft 365, GitHub, Adobe Acrobat), publicly available sources, or internal or interagency data. The systems may also generate and include limited metadata such as user IDs, timestamps, and activity logs for security monitoring.

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

AI Services may utilize commercial or publicly available information during system interaction by an authorized user.

2.4. Discuss how accuracy of the data is ensured.

According to OPM AI policy, users are responsible for inputting data appropriate to a given task and reviewing and validating AI-generated outputs before use in decision making.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Any privacy risk is limited because OPM deploys AI tools in a closed system environment and uses comprehensive monitoring tools to detect potential data loss or unauthorized disclosure of sensitive data.

Mitigation: OPM provides AI policies, Rules of Behavior, and user training. Technical safeguards, access controls, monitoring, and configuration settings further limit the types of information that can be disclosed outside of the agency.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

AI tools are broadly authorized for activities or tasks in support of official agency functions to explore increased efficiency and productivity. Such tasks and activities may include, but are not limited to drafting content, summarizing information, producing graphics, programming activities, staffing customer call centers, analyzing data, and assisting with research.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

Yes, depending on the project for which these tools are used. Any results will not be an automatic basis for decision, and output will be reviewed by a knowledgeable official before use in accordance with OPM AI policies.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Authorized OPM employees and contractors use the AI services. OCIO system administrators manage and maintain the platform.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: AI-assisted work could be misunderstood as posing privacy risks if individuals are uninformed about the protections in place governing the use of AI tools and output.

Mitigation: AI use is explained in agency governance documentation, including Rules of Behavior, relevant Privacy Impact Assessments, publicly available AI use case inventories, and OPM AI use policies.

Privacy Risk: As with other OPM information, there is a risk of inappropriate/unauthorized disclosure of sensitive information from OPM systems to external, unauthorized individuals or entities.

Mitigation: The risk is mitigated as there are clear policies, training, rules of behavior, buttressed by continuous monitoring tools that prevent risk of loss or unauthorized disclosure from agency systems.

Section 4.0. Notice

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

Users receive notice through mandatory training such as annual cybersecurity and privacy training, Privacy Impact Assessments, OPM Rules of Behavior, and the OPM system warning banner displayed prior to login.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Users cannot opt out of system monitoring or activity logging when using government systems. Access requires authentication using OPM network credentials.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware of the agency use of AI tools.

Mitigation: Appropriate notice is provided through the OPM AI policies, OPM's publicly available AI use case inventory, systems banner, Rules of Behavior, periodic IT security awareness and privacy training, and PIAs.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

User prompts, chat histories, outputs, and system activity logs are generally considered transitory or intermediary records in accordance with OPM's policies, and retained short-term to support temporary business uses, and for system functionality, monitoring, and auditing purposes. This information has a 60-day retention period, with longer retention authorized if needed for business, legal, or audit purposes.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: Privacy risk is limited. Information may be retained longer than the retention period for transitory or intermediary records if needed for official business, or for legal or audit requirements.

Mitigation: Retention of information is in accordance with OPM records management policies and relevant record schedules. Program Offices work with the Agency Records Officer to apply approved schedules where applicable.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

AI-generated content used in accordance with OPM policies shared outside OPM just like other OPM information in accordance with relevant laws, regulations, and policies.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Information is covered by the OPM Internal 3 SORN (and potentially by other relevant OPM systems of records according to the subject matter) and must be shared in accordance with the Privacy Act and other applicable laws and regulations.

6.3. Does the project place limitations on re-dissemination?

As with all agency information, users must follow applicable laws, regulations, routine uses of applicable SORN, and OPM policies when sharing AI-assisted content.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

Disclosures are logged and retained by the applicable systems and can be retrieved, as needed.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: As with other agency information, sharing information containing AI generated content is possible; however, the privacy risks are low because disclosures would be in accordance with restrictions appropriate to the sensitivity level and in accordance with the Privacy Act and other relevant laws governing disclosures outside of the agency.

Mitigation: Users must have a "need to know" to access and use privacy protected information. Also, they must review and validate AI outputs prior to use in agency decision making and follow OPM information handling policies.

Section 7.0. Redress

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

Individuals may request access to records through established Privacy Act access and amendment processes.

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

Requests to correct records are handled through the Privacy Act access and amendment processes.

7.3. How does the project notify individuals about the procedures for correcting their information?

Access and amendment procedures are published in each applicable SORN.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals may be unaware of how to correct inaccurate information.

Mitigation: OPM has published Privacy Act access and amendment processes for records access and correction for each OPM SORN.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Only officials with a "need to know" have access to Privacy Act protected information and systems access procedures are documented in OPM's policies and User Rules of Behavior. System activity is also logged and monitored by the OPM Security Operations Center (SOC) to detect suspicious activity.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees and contractors complete annual IT security and privacy training and sign Rules of Behavior.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

User access is governed by OPM access and Rules of Behavior Policies, managed through identity management processes and role-based access controls, and monitored by cybersecurity personnel.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

All MOUs and information sharing agreements, and requests for systems access or approvals for access to information are reviewed by relevant program offices, CIO officials such as the Chief Information Security Officer, and receive legal and privacy review.

Responsible Officials

Benjamin McChesney
Supervisory IT Specialist
Office of Chief Information Officer

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy