



Privacy Impact Assessment for
Collaboration Tools (CT)

October 27, 2026

Contact Point

Keith Eavenson
System Owner
OCIO/IED

Reviewing Official

Becky Ronayne
Senior Agency Official for Privacy



Abstract

Collaboration Tools (CT) is a group of cloud-based services OPM uses to transfer files, fax, send emergency and subscription messages, whiteboard, and handle help requests. CT includes Adobe Acrobat Sign, Box Secure File Transfer, Docusign IAM eSignature, eFax Corporate, Everbridge Critical Event Management, GovDelivery Communication Cloud, OPM Miro, and Zendesk. This Privacy Impact Assessment (PIA) is being conducted because CT collects personally identifiable information (PII) from users and OPM program offices use CT to send and receive files that contain PII, including through Box and Zendesk.

Overview

Collaboration Tools (CT) is a set of eight cloud-based applications that OPM staff use for everyday work with individuals inside and outside OPM. With CT, OPM staff can:

- sign and send documents electronically (Adobe Acrobat Sign, Docusign, Box);
- send and receive files securely (Box) and faxes (eFax);
- send messages to employees and subscribers, including emergency alerts (Everbridge, GovDelivery);
- plan and design together on shared online whiteboards (Miro); and
- answer questions and requests from OPM staff and the public (Zendesk).

CT itself keeps account details for its users, emergency contact details for OPM employees, and contact details for message subscribers. CT also carries the files and messages that OPM program offices send and receive. These can contain personally identifiable information (PII), such as bank statements, proof of employment, and background investigation documents. Each program office decides what it sends through CT, and its own privacy



documents cover that information. CT does not review or change file contents.

Application	What OPM uses it for	Hosting
Adobe Acrobat Sign	Electronic signatures. OPM offices sign, route, and send letters, forms, and other documents, for example to appellants, Administrative Law Judges and their paralegals, and Merit Systems Protection Board (MSPB) members.	FedRAMP-authorized SaaS, government community cloud
Box Secure File Transfer (Box)	Secure file transfer between OPM and outside parties. Box also offers electronic signatures. Signers don't log in to Box, and the signed document returns to the OPM user in Box.	FedRAMP-authorized SaaS
Docusign IAM eSignature (Docusign)	Electronic signatures and exchange of contracts and signed documents.	FedRAMP-authorized SaaS, government community cloud
eFax Corporate (eFax)	Sending and receiving faxes by email, in place of fax machines and servers.	SaaS, not FedRAMP-authorized
Everbridge Critical Event Management (Everbridge)	Emergency notices to senior leadership, continuity staff, and the OPM workforce. OPM loads every employee's contact data from active directory by Secure File Transfer Protocol (SFTP).	FedRAMP-authorized



Application	What OPM uses it for	Hosting
GovDelivery Communications Cloud (GovDelivery)	Email and text subscriptions. OPM sends announcements, workforce and operating status updates, event notices, emergency alerts, and training opportunities. Subscribers are OPM employees and outside groups such as good government groups, academia, other agencies, and the press. They sign themselves up, or program offices add them on request.	FedRAMP-authorized SaaS, hosted in the vendor's data centers
OPM Miro (Miro)	Online whiteboards for team planning, diagramming, workshops, and software design. By default, only opm.gov email addresses can create accounts. Outside users can be invited with limited access. Miro connects to tools such as Microsoft 365, Zoom, Box, and Confluence.	SaaS, not FedRAMP-authorized
Zendesk	Ticketing, self-service help articles, and automated messages that let OPM program offices handle questions and requests from internal and outside users. Appendix A lists the program office help desks ("brands") that use it.	FedRAMP-authorized

OPM users reach CT through a web browser and sign in with their Microsoft 365 account, which uses PIV authentication. Outside users reach only the content shared with them or their own account, such as Box recipients, Zendesk requesters, Miro invitees, and GovDelivery subscribers. There is no



public access to OPM-held CT data. OPM system administrators reach the services only from OPM networks or through a virtual private network (VPN).

This PIA applies to collaboration 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?

CT has no single legal authority for the information it carries. Each OPM program office that uses CT relies on the authority for its own program. Examples include technical support for the USA suite of tools, exchanges with annuitants, personnel vetting documents (including Federal background investigations), internal investigation and Office of the Inspector General records, and policy documents shared with other agencies. Questions about a specific authority go to the program office.

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

Files and messages sent through CT are covered by the SORN for the system of records where the program office keeps them. No SORN covers CT as a whole.

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

Yes.



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

No schedule is specific to CT. CT is not a permanent repository. It temporarily holds files while they are sent or received. The program office that owns a record keeps it under the NARA schedule for that record.

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.

CT collects, uses, and maintains two types of information.

Information about CT users and system operations. CT collects user account information (name, work email address, program office, and role), ticket and request details (submitter, date and time, status, and assignee), and system and audit logs (login activity, access history, and IP address). OPM staff use this information to authenticate users, route and track requests, provide support, and monitor security.

Information submitted by program offices. Program offices submit files, forms, messages, and tickets through CT. These may include bank statements, proof of employment, USA Staffing documents, personnel vetting documents, annuitant documents, and policy documents. CT maintains this information and disseminates it to the recipients the program office designates. Program offices decide what to submit and are responsible for its accuracy and retention.



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

Account information comes from the users. Everbridge employee data comes from Active Directory by SFTP. File and message content comes from OPM staff and from outside individuals, including members of the public and staff of other organizations, who upload or send it through CT.

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

No.

2.4. Discuss how accuracy of the data is ensured.

CT submit or transfer information from other sources. The person who submits information is responsible for its accuracy.

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

Privacy Risk: CT could maintain more information than is relevant and necessary.

Mitigation: This risk is partly reduced. CT do not analyze file contents. OPM authorities and procedures limit what program offices may request or send. For example, OPM does not transmit classified materials through Box. The only information CT requires is account and contact data.

Privacy Risk: Information could be collected without legal authority.

Mitigation: This risk is partly reduced. OPM policy lets CT users send or receive only information that a statute, regulation, or authority allows and that supports OPM's mission. Program office PIAs and in SORNs identify those authorities.



Section 3.0. Uses of the Information

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

OPM program offices use CT to send and receive files and messages securely, efficiently, and with an audit trail, with other agencies, partners, and the public. Account and contact data lets users sign in and lets OPM send emergency and subscription messages.

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.

No.

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

Yes. Participating OPM program offices manage and use their own licenses. OPM OCIO administers CT, reviews logs, resolves accounts problems.

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

Privacy Risk: Users could use information sent through CT inappropriately, including for purposes other than why it was provided.

Mitigation: Access is limited to individuals with a documented need to know, based on their designated role. Audit logs record anomalous system behavior.

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.

CT does not give notice to individuals. It collects only the account data users need to sign in. Program offices give any notice about the files they collect, in the CT application or by other means. OPM users also see an OPM warning



banner before they sign in that says users have no right to privacy on government systems and that OPM may monitor their activity for security and administrative purposes. CT applications also tell users that an OPM administrator may monitor conversations and activity.

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

Users generally cannot choose to leave their information out of CT. OPM users must sign in with their OPM credentials and follow OPM rules for government systems. Outside users can decline by not creating an account or not using the application. The system also records usage data, such as requests, interactions, and activity logs.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: CT users may not be able to consent to how OPM uses their information.

Mitigation: Outside users can decline by not creating an account. OPM users get notice through the warning banner and the Rules of Behavior they must accept. Other people get notice through this PIA, any applicable SORN, and the program office that collects their information.

Section 5.0. Data Retention by the Project

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

CT retains files and tickets for the periods below, then deletes them automatically:

- Box files: deleted after one year.
- Zendesk ticket attachments: deleted after 90 days.
- Zendesk tickets: archived 120 days after closing and deleted one year after closing.



These times apply only to CT. The program office that owns a record keeps its official copy under the retention schedule for that record.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: CT could keep information longer than necessary.

Mitigation: This risk is partly reduced. Automated deletion removes files and tickets. Program offices keep official records in their own repositories under NARA-approved schedules.

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.

Yes. Program offices use CT to send and receive files with other federal agencies, appellants, Administrative Law Judges, MSPB members, annuitants, applicants, and the public. Recipients see only the files and messages sent to them. CT vendors host the data under contract. Program offices' own privacy documents describe the specific recipients and uses.

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

Each program office must share information only as its own SORN allows. CT adds no sharing of its own.

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

No. OPM cannot control a file after it is sent to an outside user. OPM controls files it receives only on the OPM side.

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

Audit logs record file activity, including files sent and received.



6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information could be shared outside the scope of the SORN, without authority or without an accounting.

Mitigation: This risk is partly reduced. All OPM CT users take annual privacy awareness training. External parties who receive PII under a routine use are subject to Privacy Act limitations on disclosure and must use it consistently with the SORN. Audit logs support the accounting. OPM cannot limit the re-sharing of records released under FOIA.

Section 7.0. Redress

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

Users can view their profile and the files available to them, such as files they are sharing or receiving. To request records a program office holds, individuals follow the program office's SORN and OPM Privacy Act procedures available at opm.gov/privacy.

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

Users can correct their name, email address, and phone number in their profile. For information in files, the individual contacts the program office that owns the record.

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

CT is not a system of record for the files it holds. The program office notifies individuals about correction procedures through its SORN.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals may not know how to request access to or correction of their records.



Mitigation: OPM publishes its Privacy Act and FOIA procedures. CT does not change official records, so each program office's record correction process remains the way to fix errors.

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?

CT sends audit logs to OPM's Microsoft Defender for Cloud. The OPM Security Operations Center (SOC) reviews them in real-time for suspicious activity and takes action as needed. If the application's logs are not sent, the SOC can request them.

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

All OPM employees and contractors take IT Security and Privacy Awareness training every year and sign OPM's Rules of Behavior. Each application also has vendor documentation.

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

OPM employees and contractors sign in through Microsoft 365 single sign-on with PIV. Access is role-based. Program offices manage their own licenses, and OCIO administers CT. Outside users create accounts or are invited by an OPM user, and can only see what is shared with them.

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?

CT has no program-specific information-sharing agreements; hosting vendors operate under separate contracts. New information sharing, uses, and access are managed by the administering program office.



Responsible Officials

Keith Eavenson
System Owner
OCIO/IED

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy



Appendix A

These program office help desks use Zendesk:

- Policy Solutions
- Reasonable Accommodation
- Recruiter
- Retirement Services BODO
- Retirement Services Survey
- Staff Acquisition Applicant Support
- Suitability Executive Agent
- U.S. Office of Personnel Management
- USA Data
- USA Hire
- USA Hire Agency Resource Center
- USA Hire Interview Resource Center
- USA Learning
- USA Performance
- USA Performance – Admin
- USA Staffing
- USA Staffing Advisory Board Resources
- USA Staffing Application Manager
- USA Staffing Hiring Manager
- USA Staffing New Hire
- USAJOBS
- USTF RA
- Vendor & Agency Partners