PRIVACY IMPACT ASSESSMENT—JULY 2022

Microsoft Cloud / Office 365 General Support Services (GSS) PIA

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Provide administrative general support services for CFPB staff.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Generally applicable: Appropriate opportunities for notice, consent, access, and redress.

cfpb Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the Act), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau (CFPB). In executing its duties, the CFPB performs several daily administrative business activities such as internal and external email communications, online communications via chat and virtual meetings, calendar management, internal document development collaboration, and document and data storage. The CFPB uses three Microsoft cloud service offerings (Microsoft 365, Microsoft Azure, and Microsoft Power Platform) within the Microsoft Government Community Cloud (GCC) (herein referred to as Cloud Office) to centrally manage and automate these administrative business activities.

The CFPB Cloud Office is a third-party software as a service (SaaS) hosted by Microsoft and used by CFPB as general support system (GSS). CFPB subscribes to the use of Cloud Office to provide its employees and contractors with software applications such as:

- Microsoft SharePoint Online: Secure cloud data storage that allows document organization, sharing, and quick and efficient information access for greater collaboration and co-authoring of documents and related tasks.
- Microsoft OneDrive: A personal cloud file storage area that allows CFPB staff (i.e., employees, contractors, detailees, volunteers) to store, share, and collaborate on documents.
- Microsoft Office 365 web apps: Commonly used word and data processing, and project management tools such as Word, Excel, PowerPoint, Project, and One Note.
- Microsoft Visio: A tool that allows free form drawing of diagrams to include flowcharts, organization charts, data flow diagrams, process flow diagrams, and business process modeling.
- Microsoft Planner: A tool that provides a visual way to organize team collaboration and manage tasks and updates, to include planning new tasks, task assignment, file sharing, and chat.
- Microsoft Exchange (email): CFPB's enterprise email system for internal and external communications.
- Microsoft Teams (also referred to as Teams): A collaboration tool that features chat, voice calls, video calls and meeting facilitation and recordings, and Teams channels for collaboration on tasks and projects to support internal and external collaboration.

Microsoft Teams connects with Microsoft SharePoint, OneDrive, and Exchange to allow users to work seamlessly between these applications.

- Microsoft Stream: A video service that provides a secure way to upload, view, and share videos, to include records of meetings, presentations, and training sessions. Stream can be used within other applications such as Microsoft Teams, SharePoint, and PowerPoint.
- Microsoft Forms: A tool that allows internal CFPB staff (to include employees, contractors, detailees, interns, and vounteers) to create surveys and polls to collect feedback, organize team events, and create quizzes.
- Power Platform: A suite of tools (including Power Apps, Power BI, and Power Automate) that allow CFPB users to develop applications, build automated business solutions to analyze and draw data visualizations, or automate a business process within Microsoft Cloud. Routine tasks associated with Power Platform may include automation of workflows for approval of documents, automated organization of tasks to support document generation, and scheduling automated reminders for deadlines or re-occurring task requests.
- Whiteboard: Provides CFPB users with a virtual whiteboard that can be used for collaboration to share ideas and build solutions.
- Microsoft Bookings (Bookings): A tool that supports coordination of scheduling and booking appointments to coordinate multiple calendars, assign roles for leading and contributing to meetings, and schedule new meetings. Bookings is available with a CFPB Microsoft Exchange account and integrates with Microsoft Teams.
- Microsoft Defender: Includes Defender for Cloud Apps, Defender for Office 365, Defender for Endpoints, and Defender for Identities.
- Microsoft Azure AD: A centralized identity management repository for provisioning access to all Microsoft services.
- Microsoft Azure: Microsoft's cloud computing platform. It provides a range of cloud services, including compute, analytics, storage and networking. CFPB can pick and choose from these services to develop and scale new applications or run existing applications in the cloud.

In addition, CFPB evaluates and implements similar tools to enhance general administrative operations and functions, along with tools that further secure the environment. Cloud Office and its applications are available and accessible on CFPB provisioned laptops and cell phones to

provide general environment tools such as data storage, software maintenance such as software security patches, application upgrades, back up of data within the environment, and access management tools. Cloud Office provides these services based upon the CFPB's selection and approval of applications within the Microsoft Cloud infrastructure.

Authorized CFPB program managers, business owners, system developers, system owners, and other internal CFPB users can access Office Cloud applications to conduct normal administrative business functions such as email communications, meetings, conferencing, file sharing, and document repositories. Cloud Office applications are managed through CFPB's Change Control Board (CCB) processes and Assessment and Authorization (A&A) documentation. Privacy is addressed within application development to include functional requirements analysis, data governance reviews, detailed design reviews, alternatives analysis, feasibility analysis, benefits/cost analysis, and privacy risk assessments for each Cloud Office application.

Use of Cloud Office includes the collection and use of personally identifiable information (PII) from consumers or other members of the public, external partners and stakeholders, and CFPB staff. PII may be collected and used through email and through development of forms or documents in Microsoft Office, and PII may be stored within applications such as SharePoint. The type and scope of PII collected and used varies depending on the use case and the applications that support each use case.

The CFPB's use of Cloud Office is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. In addition, Cloud Office collects PII in accordance with, and is compliant with, the Federal Information Security Modernization Act (FISMA), the Paperwork Reduction Act, the Right to Financial Privacy Act, and the Privacy Act of 1974. The use of Cloud Office is also subject to the terms and conditions set forth in CFPB's subscription contract with Microsoft as the vendor for use of Cloud Office and its applications. The contract describes service level agreements for the ongoing maintenance of the cloud environment and licenses provided to CFPB users of its applications.

Cloud Office connects with other CFPB-authorized third-party cloud system environments, such as the CFPB's Amazon Web Services (AWS) and CFPB's Salesforce Platform[1] to support document management, data storage, and collaboration of business processes. Such connections allow data

[1] Please see the Salesforce Platform Cloud PIA found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

within Cloud Office to be used within other CFPB-authorized cloud environments, and allow documents to be stored within Cloud Office to reduce the cost of data storage. All Cloud Office interconnections to other third-party cloud systems are assessed in accordance with CFPB's A&A processes to ensure risks are identified and mitigated prior to use of either environment.

The CFPB conducts this privacy impact assessment (PIA) to assess its use of Cloud Office, its general system support (GSS) use cases, and the privacy risks associated with the development and implementation of applications with this environment and with connections with other external cloud environments and applications. The scope of this PIA is limited to the privacy risks and technical controls associated with the maintenance and use of data within Cloud Office and data that moves through interconnections with other cloud environments. Specific use cases and applications developed within Cloud Office, and the analysis of the collection and use of PII, are assessed and documented within program PIAs as necessary[2]. The CFPB's authority to collect specific information, and routine uses of those records, are identified in the associated Systems of Records Notices (SORN)[3]. Program specific uses of data that require Paperwork Reduction Act approval will also be documented within the corresponding program specific PIAs.

Privacy Risk Analysis

The primary risks identified in this PIA are the following:

- **Purpose of Collection**

Cloud Office is a GSS and CFPB's primary means of business communication through applications like Microsoft Exchange (email), Microsoft Forms, and Microsoft Teams. These applications allow the CFPB to collect and use PII from multiple sources that include CFPB employees, contractors, detailees, interns, and members of the public. Microsoft Cloud also provides environment tools and capabilities that can conduct dynamic analytics, such as Microsoft Power Platform. There is a risk that the CFPB leverages these applications to use and share PII beyond the intended purpose of its collection, and that disparate data sources may be combined and used in new ways.

[2] Program specific PIAs that address the specific uses of data within the Cloud Office environment can be found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[3] Please see https://www.consumerfinance.gov/privacy/system-records-notices/ for a list of SORNs.

The CFPB mitigates this risk through governance processes that must be followed for any intended uses of Cloud Office applications. This allows CFPB to assess new or modified capabilities to identify privacy risk. The CFPB identifies and documents how PII is collected, the purposes of those collections, and the authorized uses of PII in system and application specific PIAs that can be found on the CFPB's website. CFPB staff who use Cloud Office applications to collect, use, share, maintain, and disseminate PII are made aware of their roles and responsibilities through annual and role-based training for protecting PII.

- **Limits on Uses and Sharing of Information**

Cloud Office applications such as Microsoft Exchange (email) and Microsoft Teams are used to communicate and collaborate with external and internal individuals. As Cloud Office applications are fully integrated, PII stored within other applications such as Microsoft SharePoint or OneDrive can be shared within email and virtual meetings. While this provides a convenient way to collaborate, PII could potentially be exposed to unauthorized individuals. This risk is mitigated by configuring security controls at a granular level within each application to prevent sharing of data externally. For example, CFPB disables external sharing within SharePoint and OneDrive, prohibiting any linked document from being opened outside of the CFPB environment. Additionally, controls are in place for Microsoft Teams to prevent links posted within a virtual meeting chat from being opened externally. Furthermore, CFPB disabled the document share feature on Teams for external meetings.

Cloud Office connects with other CFPB cloud environments for the purpose of sharing and storing data. There is a risk that PII stored within another cloud environment may be accessed by an unauthorized individual or that a breach within the cloud environment may impact Cloud Office applications. The CFPB mitigates this risk by sharing PII only with systems and applications in our cloud environments that have achieved an Authority to Operate (ATO). Additionally, role-based environment and application specific access controls are implemented to ensure the security and privacy of each interconnection. Any proposed data sharing between the cloud environments is also assessed to ensure only authorized individuals can access data within Cloud Office.

- **Security**

Given the content and sensitivity of information transmitted and stored within Cloud Office, its applications may be a target for unauthorized access and/or risk insider threats. Cloud Office and its applications are therefore subject to the appropriate technical, physical, and administrative controls issued by the National Institute of Standards and Technology (NIST) to identify, analyze,

and prioritize, remediate risks. It is through this process that controls such as encryption for data maintained within the system are implemented to reduce overall risk to the data within the system. Security and privacy controls are implemented at the application level to restrict access to PII to authorized individuals, such as data loss prevention tools (DLP) to monitor and detect PII while in transit and at rest. CFPB also has implemented security tools such as Microsoft Defender that can be configured to scan Cloud Office applications to detect malware, phishing, spam, and unsafe links.

- **Individual Participation**

Microsoft Cloud is a GSS, presenting a risk that once PII is collected by an application within the environment, the PII may not be easily accessible or retrievable by the individual. This risk is addressed by the CFPB through clearly stating in privacy notices, PIAs, and SORNs the process for individuals to review of their data, request an amendment of their information, or delete their information as appropriate. Further, CFPB programs and staff that use Office Cloud applications to collect, use, and share PII identify these practices within program and system specific PIAs and SORNs. The CFPB provides individuals the ability to request access to their PII maintained in its systems of records through the Privacy Act Request process[4].

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

Privacy Risk Management

1. Describe what information the CFPB collects, how the information is collected, and the sources from which the information is collected.

Cloud Office is primarily used as a GSS to facilitate the collection, maintenance, sharing, and dissemination of information that may include PII. CFPB staff may use Cloud Office applications to facilitate the collection of PII from sources such as:

- Consumers and other individuals who conduct business with CFPB;

[4] Please see "Amending and Correcting Records Under the Privacy Act" available at https://www.consumerfinance.gov/privacy/amending-and-correcting-records-under-privacy-act/; "Submit a FOIA or Privacy Act Request," available at https://www.consumerfinance.gov/foia-requests/submit-request/.

- Internal or external stakeholders who communicate or collaborate through email or through meetings regarding CFPB business;
- CFPB staff to fulfill administrative and human resource related functions; and
- Members of the public who submit PII to the CFPB as part of a specific business purpose.

The specific PII collected varies depending on the specific purpose, and may include PII such as:

- Full name;
- Organization or associated entity;
- Personal or financial institution information;
- Contact information, including phone number, email address, and mailing address);
- Biographic and/or demographic information, including but not limited to military service history, place or birth, date of birth, race/ethnicity, citizenship and/or resident status.
- Copies of identification such as passport or driver's license;
- Employment information, such as position/title and employer's address; and
- Message log information (including IP address of sender, date, and time).

The CFPB provides Cloud Office access to CFPB staff to support internal and external communication and collaboration, and internal file sharing, document and data storage. The PII collected through Cloud Office applications varies depending on specific program use and the type of application used by CFPB staff. For example, a CFPB program staff may use Microsoft Exchange to request PII to create a Microsoft Teams video and audio meeting. PII may be recorded through Teams during the meeting or through notes transcribed in Microsoft Word. The PII contained in Teams recordings or Word documents may then be stored on Microsoft SharePoint and then shared with other CFPB staff who have a need to know. CFPB only records internal meetings with explicit approval and notice is provided prior to recording any meeting.

The CFPB assesses each program specific collection containing PII to ensure there is appropriate legal authority for the collection, and that the PII collected is the minimum amount required to complete program objectives. Cloud Office provides environment tools and applications that allow the CFPB granular control of PII, such as controls to restrict access to Microsoft SharePoint sites, libraries, folders, and files to those with a need to know. The type of PII that CFPB collects, the sources of those collections, the uses of PII, and how PII is minimized to the amount necessary

are identified in system and application specific PIAs that can be found on the CFPB's website[5]. These systems and applications may refer to the use of Cloud Office applications as a GSS to facilitate the collection, use, sharing, maintenance, and dissemination of PII, as described within this PIA.

As a result of this assessment the CFPB Privacy team is now part of governance and project working groups to assess privacy implications with the use of Microsoft tools and components within the environment.

2. Describe CFPB's objective for the information.

The CFPB uses Cloud Office as a GSS to and collaborate and communicate on a wide variety of administrative and program activities. CFPB programs that use Cloud Office applications are responsible for documenting the authority to collect and specific uses of PII and provide sufficient details around the objectives for using PII. These objectives include:

- Engage with CFPB staff and members of the public;
- Support electronic documentation creation, sharing, and storage;
- Provide secure cloud storage of data;
- Deploy security tools that protect data and uses of Cloud Office;
- Provide secure video services that allow employees and contractors the ability to record, upload, view, organize, and share video to facilitate program activities;
- Develop applications to meet business needs, including providing productivity applications, automating existing manual processes and workflows, and analyzing data; and
- Provide Cloud Office applications on CFPB provisioned mobile devices.

The CFPB assesses the design and purpose of systems and applications that collect and use PII to verify the CFPB has an authorized purpose to collect and use the information. Detailed design documents are created and reviewed to determine how IT systems such as Cloud Office collect and use PII. Any risks to PII resulting from the specific uses of Cloud Office are documented within program specific PIAs. Program specific PIAs may refer to the use of Cloud

[5] Please see https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

Office applications as a GSS to facilitate the collection, use, sharing, maintenance, and dissemination of PII as described within this PIA. Specific uses of PII are considered when applications are introduced within Cloud Office, and each data element is evaluated by the Bureau to verify that it is relevant and necessary for use. Program-specific PIAs may be completed as necessary to ensure uses of PII are assessed for risk.

3. Describe how CFPB shares any of the information with third parties with whom the CFPB shares the information for compatible purposes, e.g., federal or state agencies, the public, etc.

CFPB may collect and maintain PII within the Cloud Office applications which may enable CFPB to share PII (e.g., via email). However, CFPB only shares PII if legally authorized, and only in accordance with the routine uses published in the SORNs.

The sharing of PII with third parties using Cloud Office is documented within program specific PIAs. Program specific PIAs may refer to the use of Cloud Office applications as a GSS to facilitate the sharing of PII as described within this PIA. The CFPB documents the routine uses of information sharing with SORNs, Privacy Act Statements, and within in application specific PIAs available at www.consumerfinance.gov/privacy.

4. Describe what opportunities, if any, individuals to whom the information pertains must (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

CFPB provides notice on the collection and use of PII through the publication of this PIA, associated SORNs, and Privacy Act Statements and notices, as applicable. When practicable and/or required by law, the CFPB provides notice of the uses of PII and the opportunity to consent to uses at the time of collection. When CFPB uses Cloud Office to collect PII, notices are placed upon Cloud Office applications to the extent possible through embedded privacy statements on notice banners, web forms, email, and on forms used by individuals attached to email submissions. For example, external participants who participate in CFPB's Microsoft Teams meetings are provided notice if a meeting is going to be recorded and may choose not to participant in the meeting or remain on mute and/or off camera if there are concerns.

CFPB provides individuals the ability to request access to and amend their PII in accordance with the Privacy Act and CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 *et seq*. Information about

Privacy Act requests is published in SORNs associated with systems that contain system of records (and the PII within them) found at https://www.consumerfinance.gov/privacy/system-records-notices/. Individuals may be able to directly update their information – for example, by contacting the CFPB directly to update contact or mailing information, or updating information previously emailed by an individual to a specific program or office.

5. Explain the standards and relevant controls that govern the CFPB's—or any third-party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

The CFPB conducts full security reviews of Cloud Office based on all applicable federal laws, directives, and standards. The CFPB develops and follows a Security Implementation Plan (SIP) identifying the necessary procedures governing the use of PII within the environment. The Cloud Office environment maintains an Authority to Operate (ATO) that acknowledges that appropriate security and privacy controls are in place within the environment. Some users may also include authorized CFPB contractors. All users are required to complete CFPB annual and role-based privacy and security training prior to gaining access to Cloud Office applications. Privacy is carefully considered to ensure PII use within its application is in alignment with the CFPB's authority to collect, use, maintain, and share PII. Privacy reviews are part of each application design, and part of any changes, modification, or upgrades to the Cloud Office environment to assess whether any changes present privacy implications.

The CFPB's use of Cloud Office, and its applications, involves the appropriate security and privacy controls that are implemented, tested, and reviewed as part of the agency's information security and privacy programs. These services are subject to the Federal Information Security Modernization Act (FISMA) implementing standards and the most current CFPB regulation guidance.

Cloud Office provides CFPB with integrated application workflows, personal data storage (Microsoft OneDrive), overall data storage (Microsoft SharePoint), tailorable templates such as forms, dashboards and reports, and business intelligence tools; and it provides the network, system management, and application security software that is configurable at a granular level within each application. CFPB assesses the use of each these technologies to determine risk associated with each program-specific use of Cloud Office applications. The capabilities that Cloud Office provides require consistent risk management and continuous monitoring processes maintained by the CFPB's Security and Privacy Continuous Monitoring Strategies, allowing for

consistent and substantive reviews of security and privacy controls to ensure the security of the environment and privacy of the data residing within it.

The CFPB leverages Cloud Office as a GSS to support several business operations and program activities. When a program leverages Cloud Office applications as part of its data collection and use, CFPB reviews detailed design documentation to ensure design feasibility and to complete necessary security and privacy compliance requirements prior to implementing the system for use. As a result of this PIA, Cloud Office been assessed to determine how its applications provide a more secure, automated approach for business operations. The following technical and administrative controls have been identified to secure PII and to create accountability for the CFPB's appropriate collection, use, disclosure, and retention of the information:

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to Cloud Office applications, and to the data that resides within those applications.
- Specific policies and procedures that govern the Cloud Office environment, such as procedures for requesting and approving access to applications within the environment.
- Completion of CFPB's role-based privacy training is required prior to granting access to Cloud Office applications. In some cases, applications such as Microsoft Exchange (email) and role based training includes topics such as data handling procedures, incident and breach response procedures, and the CFPB's authority to collect and use information in accordance with its regulations.
- CFPB incident response procedures and privacy breach response procedures are in place to address incidents involving data residing in Cloud Office applications.
- Compliance with CFPB cybersecurity policy and procedures are documented within security and privacy implementation plans.
- Governance procedures are in place for tools like Microsoft Power Platform that allow users to create applications. These procedures review the detailed design and proposed data uses to ensure that security and privacy risks are addressed with applicable controls.
- Microsoft 365 provides security tools within its environment that allow granular security control configurations to be customized for each application. The baseline configurations include anti-malware, anti-phishing, anti-spam, safe link monitoring, and safe attachment scans.
- Mobile device management is installed on CFPB provisioned mobile devices to restrict and monitor Cloud Office applications.

- Data loss prevention (DLP) tools are provided through Microsoft Office to monitor exfiltration when applications are used to communicate externally.
- Role-based Access Controls: The CFPB is responsible for assigning and maintaining roles and permissions within Office Cloud and its applications based on an individual's role within the organization and as approved by Cybersecurity. The following lists examples of the roles and responsibilities within Microsoft Office:
    - Microsoft Support – Authorized Microsoft employees and contractors who are available to CFPB to support troubleshooting and general administrative support described within CFPB's contract with Microsoft.
    - System Administrator and System Administrator roles - These are performed by authorized CFPB employees and contractors. These roles have full access to manage security configuration settings within the Cloud Office environment, including management of user account privileges and permissions. Security controls such as session time-outs or log out after a period of inactivity.
    - Exchange Administrator roles: Performed by CFPB employees and contractors to assign the need to view and manage user's email mailboxes, Microsoft 365 groups, and Exchange Online.
    - Password Administrator role: CFPB employees and contractors use this role to manage passwords for non-administrators.
    - User Administrator role: Roles used by CFPB employees and contractors to set up and manage usernames, delete and restore user accounts, and change user passwords.
    - CFPB Basic User roles - This role is assigned to all CFPB staff who are granted access to application(s) in Cloud Office. Permissions are based upon assigned business function (e.g., Contracting Office Representative (COR), program manager, project manager, developer, administrator, etc.) and security configurations are based on their business and security needs within a specific application.
    - Service Account roles - Service accounts roles are specific non-system administrator user accounts assigned to authorized CFPB employees and contractors that are used for data synchronization, managing API credentials, and to synchronize identity information.

- Records Schedules submitted to and approved by National Archives and Records Administration (NARA) are in place for each collection of data at the application level. Applications that collect, use, maintain, and/or share PII may retain records indefinitely until the NARA approves the CFPB's records disposition schedule. Records that fall under a general records schedule are maintained and disposed of according to the applicable schedule identified within program specific PIAs and SORNs.
- Data quality and integrity checks to continually validate that PII within the Cloud Office is accurate and relevant for the purposes it was collected for.
- Extract logging and reviews to ensure that applications within Cloud Office is only used by authorized CFPB staff.
- Federal Committee on Statistical Methodology Government-wide Statistical Standards
- Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies
- Personnel Security including background checks are completed for all employees, contractors, or other individuals authorized to complete CFPB activities within Cloud Office applications.

Program specific technical and administrative controls to secure PII and to create accountability for the CFPB's appropriate collection, use, disclosure is further documented in program specific PIAs. The CFPB may use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA, and those contractors are subject to similar controls. Contractors with access to PII are required to report suspected or confirmed privacy incidents to the CFPB immediately and no later than one hour after discovery. Other requirements placed on contractors may include training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations (FAR).

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the CFPB, e.g., government contractors discussed in Question 5.)

Cloud Office connects with other CFPB-authorized and managed third-party cloud environments such as AWS and Salesforce. These connections provide increased collaboration, improved coordination, increased security, reduced data storage needs and associated costs, and additional

data analytics and visualization capabilities. For example, Cloud Office connects with Salesforce to allow CFPB staff to use data collected from Salesforce applications within SharePoint for real-time document collaboration, reducing the need to manually download, attach, and email attachments. The CFPB connects Cloud Office with other third-party tools such as Splunk to monitor logs from applications like email to detect unauthorized access or suspicious activities. The CFPB also connects internal and external applications, data, and devices with integration tools like MuleSoft, which allows CFPB to create reusable application programming interfaces (APIs) to move information between systems and environments, such as interconnections between Salesforce and Microsoft SharePoint. These connections are secured using both Salesforce and Cloud Office access controls such as Microsoft's Azure Active Directory solution and conditional access policies.

All Cloud Office applications are subject to a project governance lifecycle where the scope and uses of each application are assessed by the CFPB's security and privacy teams to ensure compliance with CFPB policies and procedures. This includes any applications that connect with other third-party environments or application. All third-party tools and service providers contracted by CFPB must also be assessed in accordance with a Security and Privacy Implementation Plan (SIP) identifying the necessary controls that must be in place and achieve a separate ATO prior to connection with Cloud Office. Depending on the type of connection, and the environment that Cloud Office connects to, typical controls include:

- Memoranda of understanding, information sharing agreements, and risk assessment memoranda describing the collection, use, maintenance, and sharing of any PII contained within Cloud Office;
- Documented compliance with CFPB cybersecurity policy and procedures;
- Audit logs and reviews policy and standard operating procedures; and
- Role-based access controls.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2022.07.20 17:15:04 -04'00'

Chris Chilbert

Chief Information Officer

Date

TANNAZ HADDADI

Digitally signed by TANNAZ HADDADI
Date: 2022.07.20 17:35:28 -04'00'

Tannaz Haddadi

Chief Privacy Officer

Date

Kathleen Barrett

Katy Barrett

System Owner

Date

Change control

Version	Summary of material changes	Pages affected	Date of change
1.0	Initial PIA draft		
1.1	Final Draft		