Salesforce Platform (Cloud Environment)

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Provide a platform as a service (PaaS) cloud environment to build and maintain applications supporting various operational activities.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Opportunities for notice, consent, access, and redress are documented in program-specific PIAs and SORNs.

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 consumer and stakeholder relationship management and internal employee collaboration activities through a variety of business processes that are supported by information technology (IT) systems and applications. The CFPB uses Salesforce, Inc. (Salesforce) cloud services to modernize its IT portfolio to increase the efficiency and effectiveness of its consumer service management business processes and to decrease the cost of hardware and software required by traditional systems and applications to support those business processes.

Salesforce is an external, Platform as a Service (PaaS) cloud-based customer relationship management platform offering extensive options for configuring workflows, databases, forms, dashboards and reports, process modeling, and customizable user interfaces. Salesforce provides a selection of 'out of the box' functionality and custom tools to build internal and external facing applications that support various efforts such as consumer engagement and outreach, relationship management processes, employee collaboration, and internal workflows. Salesforce enables the CFPB to quickly and efficiently build secure applications that automate manual business processes. These processes may involve the collection of personally identifiable information (PII) from consumers or other members of the public, external partners and stakeholders, and CFPB staff. The type and scope of PII collected varies depending on the use case.

The CFPB's use of Salesforce is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. In addition, specific CFPB programs use and collect PII through Salesforce in accordance with legal authorities under which the programs operate. Information in Salesforce is collected in accordance with and is compliant with the Paperwork Reduction Act, the Right to Financial Privacy Act, and the Privacy Act of 1974. The use of Salesforce as a third-party cloud environment is also subject to the terms and conditions set forth in CFPB's contract with Salesforce as the vendor, to include the provisioning of the environment, service level agreements for the ongoing maintenance of the environment, and licenses provided to the CFPB for use of the environment.

Salesforce manages CFPB's technical cloud infrastructure on behalf of the CFPB, including general cloud environment tools such as data storage, system computing resources (such as routers and firewalls, data centers), software maintenance (such as security patches and secure upgrades to the environment), and access management tools. Salesforce provides access to its

environment tools and services to CFPB to build systems and applications to facilitate customer service business processes, including:

- The collection and use of data via phone, web forms, chats, or email allowing the CFPB to quickly connect and solve consumer cases or complaints.
- The collection of data such as applications for CFPB advisory boards and committees.
- Integrated, prebuilt case management tools and capabilities allowing the CFPB to handle case management activities such as scheduling of meetings and interviews quickly and efficiently.
- The ability to integrate data held within transitional data systems and databases, saving the CFPB time and resources otherwise spent on data migration activities.
- Ability to build applications that the CFPB uses to automate Helpdesk ticket resolution, escalate consumer concerns and complaints, and resolve consumer issues and concerns.
- Standardized data collection methods and processes, such as standardizing the format of mailing addresses and customization of form fields, to collect the same type and amount of data to reduce duplicative and incorrect information.
- CFPB authorized internal and third-party tools offered within the environment (referred to as AppExchange) to support system development, administration, maintenance, and data storage.

CFPB Salesforce data is hosted and stored in the Salesforce Government Cloud, which is a Compliant Cloud System with Agency Federal Risk and Authorization Management Program (FedRAMP) High Authorization. Salesforce also integrates with other CFPB-authorized third-party cloud system environments for purposes such as the storage of data. The integration allows data within Salesforce to be archived and stored securely within other CFPB-authorized cloud environments to reduce the cost of data storage, scan data and documentation to determine threats such as viruses prior to upload, and system security logging and monitoring tools to ensure authorized access to the environment. All third-party cloud systems that connect with Salesforce are assessed according CFPB's assessment and authorization (A&A) processes to ensure risks are identified and mitigated prior to use.

Authorized CFPB program managers, business product and system owners, system developers and business analysts, and other internal CFPB stakeholders and users can access Salesforce to leverage these technical capabilities to build systems and applications in a secure, consistent method. Salesforce, and applications developed within Salesforce, are managed through the CFPB

Enterprise Platforms Salesforce Center of Excellence (COE), CFPB Change Control Board (CCB) processes and A&A documentation and addresses privacy relative to systems development to include functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and privacy risk assessments.

The CFPB conducts this privacy impact assessment (PIA) to assess its use of Salesforce and identify the general system support use cases and the associated privacy risks The scope of this PIA is limited to the privacy risks and technical controls associated with the maintenance and use of data within Salesforce. Specific use cases and applications developed within Salesforce, and the analysis of the collection and use of PII, are assessed and documented within program specific PIAs[1]. The CFPB's authority to collect specific information, and routine uses of those records are identified in the associated Systems of Records Notices (SORN)[2]. 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**

Salesforce allows CFPB to automate manual tasks, collect and use data from multiple sources that include CFPB employees, contractors, detailees, interns, and members of the public. Salesforce also provides environment tools and capabilities that can conduct dynamic analytics, allowing data to be used for different purposes at the CFPB's discretion. There is a risk that the CFPB leverages these advantages to use data beyond the intended purpose of collection, and that disparate data sources may be combined and used in new ways that are not consistent with the initial collection. The CFPB mitigates this risk by conducting program specific PIAs to assess the collection and uses of PII in accordance with the authority to collect PII. The CFPB addresses privacy implications during the development lifecycle of an application to ensure that this privacy

[1] Program-specific PIAs that address the maintenance and use of data within the Salesforce environment include the Scheduling and Examination system and the Legal Division Matter Management system found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[2] Please see https://www.consumerfinance.gov/privacy/privacy-impact-assessments/ for a list of CFPB PIAs and https://www.consumerfinance.gov/privacy/system-records-notices/ for a list of SORNs.

risk is managed throughout the development lifecycle, and continuous monitoring on systems and applications to ensure the purpose of collection remains consistent.

- **Openness and Transparency**

Salesforce provides a suite of standardized tools and components that are native to the Salesforce environment. CFPB uses these tools to develop several applications within the environment, each with a specific collection and use of data, to include PII. There is a risk that individuals do not understand the functionality of Salesforce and how their data is used by applications within the environment. The CFPB mitigates this risk through Privacy Notices, Privacy Act Statements, PIAs and SORNs to help individuals understand the purpose of Salesforce and describe how their PII is collected, used, shared, and maintained within the environment. Included within these documents are ways in which individuals can contact the CFPB to learn about how PII is used within specific applications in Salesforce.

- **Data Minimization**

Salesforce provides the CFPB with the ability to collect PII in various ways, some of which may not be necessary for the purpose of collection. To mitigate this risk, the CFPB reviews collections of data within each application to minimize the collection of PII to the greatest extent possible, while allowing CFPB to complete its objectives. This may be achieved by stripping collections of PII, aggregating data, or other means of minimizing such collection. Nevertheless, the CFPB necessarily collects PII under its legal authorities and consequently utilizes appropriate technical, physical, and administrative controls relative to the risk of the data within Salesforce. Salesforce provides development tools and components that allow granular control of data collection options, such as the customization of data fields to limit the amount of PII entered by individuals to the minimum amount necessary. These controls are discussed below and in the appropriate PIA and SORN associated with a specific collection of PII.

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

Data within Salesforce may also be shared with other cloud environments for data storage and archival. For example, the CFPB's Amazon Web Services (AWS) environment provides a secure data storage environment that Salesforce can connect to store large amounts of data. This presents a risk that data stored within another cloud environment may be accessed by an unauthorized individual or that a breach within the cloud environment may impact business operations within Salesforce. The CFPB mitigates this risk by sharing Salesforce data only with systems that have achieved an Authority to Operate (ATO) based upon the CFPB A&A processes. Connections between other cloud environments is assessed by the CFPB to apply role-based environment

access controls to ensure the security and privacy of the interconnection. Any proposed data sharing between the cloud environments is also assessed to ensure only authorized individuals can access data within Salesforce.

- **Data Quality and Integrity**

Salesforce provides the ability to create several diverse types of applications to support a range of CFPB processes, providing the CFPB the ability to collect large amounts of information. This presents a risk that information collected over time may be inaccurate, outdated, or incomplete. Further, Salesforce allows the CFPB to customize granular access control permissions for the overall environment, and for each application within the environment. This presents a risk that access is granted inadvertently, allowing unauthorized users to access and modify data. The applications created within Salesforce collect information voluntarily, allowing an individual to provide accurate information while providing notice of collecting PII at the time of collection, minimizing the risk of inaccurate data collection. To mitigate these risks the CFPB implemented controls that restrict access to data and changing permissions to restrict changes to information by unauthorized parties, regularly backs up data that can be restored in the event of an unauthorized modification of data, and maintains audit logs to determine when data is added, modified, or deleted.

- **Security**

CFPB information is hosted on a dedicated Salesforce Government Cloud Plus environment, that has been built on an AWS GovCloud instance. Salesforce Government Cloud Plus is a Compliant Cloud System with FedRAMP High Authorization. Given the content and sensitivity of information held within Salesforce the data may be a target for unauthorized access and/or risk insider threats. Information within Salesforce is therefore subject to the appropriate technical, physical, and administrative controls implemented through the CFPB's National Institute of Standards and Technology (NIST) based risk management process that identifies risk, analyzes the risk, prioritizes the risk, and develops plan to remediate the risk. It is through these processes 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 within the Salesforce environment and are also implemented within systems and applications built within the environment to restrict access to the information to authorized individuals. Salesforce performs three major environment releases/upgrades per year: Spring, Summer and Winter. Prior to each release, Salesforce issues release notes and updates various lower environments to allow for testing. Prior to each major release, the CFPB architects review the release notes and

present findings to the CFPB Salesforce Software Advisory Group to notify developers of items that may impact the platform as well as individual Salesforce applications. CFPB architects and application developers ensure that CFPB product releases are coordinated around these major releases, and that patching, and upgrades do not affect the performance of applications or data within the Salesforce environment.

- **Individual Participation**

Salesforce at the Bureau provides access to several applications and systems that are built for CFPB purposes. Once information enters the Salesforce environment there is a risk that data may not be easily accessible or retrievable by the members of the public that provide their PII. This risk is addressed by the CFPB through clearly stating in privacy notices, PIAs, and SORNs the process for individuals to request a review of their data, methods by which an individual can request an amendment of their information or deletion of their information, or if such a request is denied the reasons for the denial in accordance with CFPB regulation, as appropriate.

- **Accountability and Auditing**

The Salesforce environment hosts a diverse set of business applications, each with its own data use cases for the collection, sharing, and maintenance of data. This leads to a risk that Salesforce maintains different amounts and types of PII used for different purposes, leading to an unauthorized individual inadvertently accessing PII. The CFPB mitigates this risk through data access controls supported by role-based privacy training for individuals who handles data. Program-specific PIAs are also completed for all applications within Salesforce that collect, use, share, and maintain data to identify roles for accessing data. Additionally, both internal and independent auditors hold the CFPB accountable for complying with CFPB policies and procedures related to the processing of PII. The CFPB is committed to taking swift and immediate action if we uncover any violations of law, policies, and procedures.

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate and implemented within the Salesforce environment and within program specific PIAs.

Privacy Risk Management

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

The CFPB uses its Salesforce applications to support a wide variety of CFPB activities. Such activities may involve collecting and maintaining PII and other related data of consumers and CFPB staff (i.e., employees, contractors, interns, detailees, etc.); individuals involved in supervisory, enforcement, or other legal matters with the CFPB, including CFPB employees and external individuals such as judges, opposing counsel, expert witnesses, arbitrators, and mediators; confidential information (CI) or other data about financial institutions; members of the public, including consumers who submit a complaint or inquiry to the CFPB; and other related routine business communications and data such as day-to-day email communications and work documents to support business functions. The PII collected by Salesforce varies depending on the specific use case; however, the information may include first name, last name, associated entity, phone number, email address, mailing address, military information (including branch, rank, location, service status), employer, position/title, employer's address, place of birth, date of birth, gender, race/ethnicity, and citizenship and/or resident status. The PII collected and used within Salesforce applications may include:

- Collection, use, and storage of PII within documents related to CFPB's examination and supervision processes.
- Creation, management, and reporting of examination and supervision case records that are managed by automated workflows created with Salesforce to allow faster analysis and decision making by the CFPB.
- Tracking, managing, and maintaining administrative schedules and calendars to support the CFPB's examination and investigative responsibilities.
- Tracking, analysis, and management of internal and external correspondence to include automated scheduling and tracking of responses to inquiries.
- Increased ability to perform trend, pattern, and correlation analysis of large data sets to provide faster consumer response, examination, and supervision processes.
- Collecting, organizing, sanitizing, and sharing data for public consumption.

Generally, Salesforce provides the CFPB the ability to build automated methods for collecting PII from individuals. For example, the CFPB can collect data from individuals through the creation of web forms, through website submissions, or by submitting data to the CFPB via mail, email, or phone that is then uploaded by Bureau staff. The CFPB assesses each program-specific collection

of data to ensure the collection falls under a legal authority to do so, and that the PII collected is the minimum amount required to complete program objectives. Salesforce provides environment tools and components that allow the CFPB granular control of data collection options, such as the customization of data fields to limit the amount of PII entered by individuals. How data is collected, the sources of those collections, and how data is minimized to the amount necessary are identified in application specific PIAs that can be found on the CFPB's website located at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

2. Describe CFPB's objective for the information.

Salesforce provides an ability to collect, process, and store PII to support a variety of CFPB programs and business functions through the development of and management of applications within the cloud environment. The CFPB's objectives include the following:

- Creating applications or forms to collect and manage feedback, correspondence, or submissions to CFPB, including but not limited to:
    - Consumer complaints or inquiries about financial products, services, and the entities providing them
    - Voluntary assessments from financial entities regulated by CFPB
    - Examinations and monitoring of bank and non-bank entities
    - Candidates' applications for positions on CFPB advisory committees, boards, or other positions
    - Whistleblower tips and contact information concerning companies or individuals that may be in potential violation of consumer protection laws
    - Individual submission of credit card agreements and survey details on behalf of an entity for CFPB analysis.
- Providing responses to external entities (e.g., consumer, industry stakeholders) who submit inquiries by email, voicemail, and web form submissions built within Salesforce.
- Providing case management capabilities to better track litigation and non-litigation cases management by CFPB's Legal Division and tracking that collects PII to facilitate matters.
- Providing a consolidated database to make inquiry management processes more efficient and providing more ways to collaborate and have insight into the inquiry management and response process.
- Providing applications to track and manage divisional and office budget and procurement actions.

When a program specific collection of data is proposed, the CFPB assesses the design and purpose of the system, to include a collection of PII, through system design documentation reviews to verify the CFPB has an authorized purpose to collect and use the information. Each program-specific use of PII is also assessed to determine the impact to privacy, and resulting risks are documented within program specific PIAs. Specific collections and methods of collection are further described in system and program specific PIAs.

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.

In instances where the CFPB may have to share PII maintained within Salesforce with third-parties, that information is only shared with consent from the impacted individuals or when CFPB otherwise has the authority to do so, and pursuant to routine uses published in our SORNs.

Generally, the CFPB may share PII with third parties such as other federal regulators or federal or state government agencies that supervise Dodd-Frank covered entities or for purposes of enforcing various related laws or regulations, in a response to a request from Congress, for a security incident involving information collected within Salesforce, or through investigative or legal process as part of litigation activities. When external users are provided access to an application within Salesforce, the CFPB ensures that these individuals are authorized by the application owner and applies strict user access controls that limit access to only the data for which they are granted access. This access is periodically reviewed to ensure only authorized individuals maintain access, and to remove access when no longer required by the application owner or the external user.

In addition, CFPB may also leverage third-party software, such as application programming interfaces (APIs), to connect Salesforce to other CFPB-authorized cloud environments such as AWS or Microsoft. In these cases, CFPB reviews the terms of use and licensing agreements of both environments prior to building an API. The API is also assessed by CFPB to ensure its application does not create risk to either environment or to the data that resides within the environments.

The CFPB documents the routine uses of information sharing with SORNs, Privacy Act Statements, and within application specific PIAs available at www.consumerfinance.gov/privacy.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (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 how we collect and use 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. These notices are located on Salesforce application-hosted webpages, web forms, electronic collections, and on forms used by individuals to submit information to a Salesforce application.

CFPB provides individuals the ability to request access and amendment to 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 the associated SORNs[3]. Individuals may sometimes be able to directly update their information – for example, by contacting the CFPB directly to update contact or mailing information, or updating information provided for registration purposes for a CFPB-sponsored event.

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 review of the Salesforce environment based on all applicable federal laws, directives, and standards. The CFPB develops and follows a Security Implementation Plan (SIP) identifying the necessary procedures to use PII within each application developed within the environment. The Salesforce environment maintains an ATO that acknowledges that appropriate security and privacy controls are in place within the environment. The CFPB issues authorized personnel access to the platform following the CFPB's User Access Request process. Some users may also include authorized CFPB contractors. All users are required to complete mandatory privacy and security training and additional training prior to gaining access to Salesforce, or within any of the applications within the environment. Users must also complete

[3] Please see https://www.consumerfinance.gov/privacy/system-records-notices/ and https://www.consumerfinance.gov/foia-requests/

the user agreement outlining their roles and responsibilities in using the system and the information contained within it. Privacy is carefully considered when applications are developed within the Salesforce environment to ensure the application design 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 Salesforce environment to assess whether any changes present privacy implications.

The CFPB's use of Salesforce 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.

Salesforce provides CFPB with out of the box information workflows, databases, tailorable templates such as forms, dashboards and reports, and provides the network, data storage, system resources, data centers, security, application software with the environment. CFPB assesses the use of each these technologies and components to determine risk associated with each program-specific use. The capabilities that Salesforce 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 develops applications within Salesforce using an agile development process 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 the Salesforce environment has been assessed to determine how its tools, components, and applications provide a more secure, automated approach for business operations. As a result, the following technical and administrative controls have been identified to secure the data 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 the Salesforce environment and to the data that resides within its applications.
- The CFPB's general Privacy training and role-based privacy training are required prior to granting access to Salesforce and any applications within the environment. 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 breach response procedures are in place to address incidents involving data residing in the Salesforce environment.
- Compliance with CFPB cybersecurity policy and procedures are documented within security and privacy implementation plans.
- Role-based Access Controls: The CFPB is responsible for assigning and maintaining roles and permissions within Salesforce 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 Salesforce:
    - 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 Salesforce environment, including management of user account privileges and permissions. Security controls such as session time-outs ask the user to continue working or log out after a period of inactivity.
    - CFPB Basic User roles - This role is assigned to all CFPB employees and contractors who are granted access to application(s) in Salesforce. Permissions are based upon assigned business function (e.g., Contracting Office Representative (COR), Examiner, Investigator, Stakeholder Support, 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.
- Personnel Security including background checks are completed for all employees, contractors, or other individuals authorized to complete CFPB activities within Salesforce.

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 direct identifying 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.)

Salesforce provides the CFPB with the ability to connect third party vendors services to the environment to support enhanced performance, increased security, data storage needs, and data analytics and visualization capabilities from its application exchange and from other CFPB cloud environments. The Salesforce application exchange is a list of available tools created within Salesforce, and approved by Salesforce as a verified partner, to support application development and performance. For example, CFPB uses applications located with the Salesforce AppExchange that can be added to applications developed within Salesforce. The CFPB may also connect Salesforce with other cloud services and tools, such as AWS, to store data securely, allowing the CFPB to leverage AWS data storage services. The CFPB connects Salesforce with other third-party tools that parse, cleanse, and standardize data, and to protect the Salesforce environment from malicious viruses that could be sourced from external individuals that submit file attachments into Salesforce applications. The CFPB also connects internal and external applications, data, and devices with integration tools like MuleSoft, which allows CFPB to create reusable network connections with 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 controls and OKTA, CFPB's enterprise identity management service.

Any applications developed within the Bureau's Salesforce environment are managed through a project governance lifecycle where the scope and design of the application is assessed by the CFPB's security and privacy teams to ensure compliance with CFPB policies and procedures, to include any tools and components selected from the Salesforce application exchange. Salesforce connections with other third-party cloud services, such as AWS, are also reviewed to ensure

compliance. Typically, third-party tools and services providers must also be assessed in accordance with a SIP identifying the necessary controls that must be and achieve a separate ATO prior to connection with Salesforce. Depending on the connection typical controls include:

- Memoranda, information sharing agreements, and authority to use describe the collection, use, maintenance, and sharing of any PII contained within Salesforce
- Documented compliance with CFPB cybersecurity policy and procedures
- Audit logs and reviews policy and standard operating procedures
- Role-based Access Controls.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2022.04.22 12:59:00 -04'00'

Chris Chilbert

Chief Information Officer

Date

TANNAZ HADDADI

Digitally signed by TANNAZ HADDADI
Date: 2022.05.05 10:19:53 -04'00'

Tannaz Haddadi

Chief Privacy Officer

Date

ADEBIMPE ABANISHE

Digitally signed by ADEBIMPE ABANISHE
Date: 2022.04.22 09:55:32 -04'00'

Adebimpe Abanishe

System Owner

Date