PRIVACY IMPACT ASSESSMENT—DECEMBER 2022

Amazon Web Services General Support System (AWS Alto) PIA

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Provides cloud-based enterprise hosting solutions for cloud-hosted systems and applications.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Appropriate opportunities for notice, consent, access, and redress.

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 or Bureau). CFPB performs a range of functions including, but not limited to, supervising and enforcing financial entities, conducting research on financial markets, and collecting and responding to consumer complaints. In support of business operations CFPB requires a flexible information technology (IT) general support system (GSS) infrastructure for hosting the development, testing, and production of systems and applications and robust data collection, storage, and processing capabilities.

CFPB uses an Amazon Web Services (AWS) environment (and herein referred to as AWS Alto), that provides Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). AWS Alto decreases the cost of hardware, software, and data storage that support Bureau business processes by providing a cloud hosted environment. As a GSS, AWS Alto provides the infrastructure to host CFPB's systems, applications, and the data used within them. AWS Alto, as a third party service provider, does not directly collect, maintain or disseminate data, but it provides the hosted infrastructure for CFPB-owned and managed systems and applications to perform business functions. AWS manages the AWS Alto environment on behalf of CFPB, including general data storage, system computing resources (such as routers, firewalls, and data centers), software maintenance (such as security patches and secure upgrades to the environment), and access management tools. AWS Alto also partners with vetted third-party vendors who provide their services through AWS' Marketplace, allowing CFPB to assess and deploy these services seamlessly within its AWS Alto to support the hosted systems and applications residing in its environment.

CFPB uses AWS Alto to build or migrate business systems and applications that directly collect, use, maintain, and share personally identifiable information (PII) as part of their operations. This data may include:

- Data collection via forms, website interfaces, secure upload web forms, and other mechanisms to support a wide variety of data collection from members of the public, supervised entities, or others.
- Database and data warehouse management and storage capabilities that save CFPB time and resources.

- Data analytic capabilities to enables data analysis and visualization of data such as reports, dashboards, and status tools that increase work productivity by replacing manual business processes.
- Web applications and web servers that support a wide variety of general online services such as CFPB's website.
- Security services such as threat detection applications that enforces security and privacy controls and continuously monitors for malicious activity to secure the environment. This also includes tools and applications that facilitate encryption and log monitoring capabilities.
- General IT network support and access management tools for managing interconnections with systems, applications, and tools.
- Applications and services that support mobile computing and connected mobile devices that can access AWS Alto.

AWS Alto hosts and connects with other CFPB-authorized third-party cloud system environments, such as CFPB's Salesforce and Microsoft Office 365 (O365) environments, to support the storage of data, data analytics, and processing of data[1]. Such connections allow data within AWS Alto to be stored securely to reduce the cost of data storage and conduct system security logging to monitor authorized access to the environment. All third-party cloud systems that connect with AWS Alto are assessed according CFPB's assessment and authorization (A&A) processes to ensure that risks are identified and mitigated prior to deployment or integration.

AWS Alto consists of production, development, staging, and sandbox environments that supports the development and migration of systems and applications. For example, CFPB uses a staging environment with AWS Alto to test operational viability of hosted business systems and applications, and to ensure that general security measures are in place for these systems and applications to collect, process and transmit data. Authorized CFPB program managers, business owners, system developers, system owners, and other internal CFPB users can leverage these technical capabilities to build systems and applications in a secure, consistent method. AWS Alto,

[1] The Salesforce Platform Cloud Environment, Microsoft General Support Services (GSS) environment, and relevant system PIAs are found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

and the systems and applications developed within its environment, are managed through CFPB Change Control Board (CCB) processes and A&A documentation.

The scope of this privacy impact assessment (PIA) is limited to the privacy risks and technical controls associated with the maintenance and use of personally identifiable information (PII) within AWS Alto. Specific use cases for systems and applications developed within AWS Alto, and the specific collection and use of PII, are assessed and documented within program-specific PIAs[2]. Program-specific uses of data that require Paperwork Reduction Act approval are also documented within the corresponding program-specific PIAs. CFPB documents the collection and use of PII in a system of records, the authority to collect specific information, and routine uses of those records in the associated system of records notice (SORN)[3]. CFPB's use of AWS Alto is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. In addition, information in AWS Alto is collected in accordance with and is compliant with the Dodd-Frank Act, the Paperwork Reduction Act, the Right to Financial Privacy Act, and the Privacy Act of 1974, as applicable.

Privacy Risk Analysis

The primary risks identified in this PIA are the following:

- **Purpose of Collection**

AWS Alto enables CFPB to collect and use data from multiple sources that include financial entities such as banks, individuals such as the public, and CFPB staff. AWS Alto also provides environment tools and capabilities to conduct dynamic analytics across multiple data sets. This creates a privacy risk that disparate data sources may be combined and used in new ways other than for the purpose for which they were collected. CFPB mitigates this risk by conducting program-specific PIAs to assess the collection and uses of PII in accordance with the authority to collect the PII. When CFPB programs choose to leverage AWS Alto for hosting systems, applications, or PII, CFPB documents the privacy implications within PIAs, as required. CFPB also addresses privacy risk throughout the development lifecycle and performs continuous

[2] Program specific PIAs that address the maintenance and use of data within the AWS Cloud are 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.

monitoring on systems and applications within the AWS Alto to ensure the purpose of collection remains consistent.

- **Openness and Transparency**

AWS Alto is a cloud-based environment in which system and application development is quick and efficient. CFPB uses AWS Alto-provided tools to develop, test, and maintain several applications within the environment. There is a risk that members of the public do not understand the functionality of the AWS environment and how their data is collected, used, and stored by systems and applications within the environment.

CFPB mitigates this risk through the use and publication of Privacy Notices, PIAs, and SORNs to help individuals understand the purpose of AWS Alto services and describe how their PII is collected, used, shared, and maintained within the environment. These documents include ways in which individuals can contact CFPB to learn about how PII is used within specific applications in AWS Alto.

- **Data Minimization**

AWS Alto provides tools that allow CFPB to collect, use, and share PII throughout its environment for business uses, and there is a privacy risk that unnecessary PII may be collected inadvertently. To mitigate this risk, CFPB reviews collections of data within each system and 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 directly identifying PII to minimum necessary, aggregating data, or other means of minimizing such collection. CFPB collects PII in accordance with its legal authorities and implements appropriate technical, physical, and administrative controls relative to the risk and sensitivity of the data within AWS Alto. AWS Alto provides application 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.

The CFPB-designed AWS Alto provides a staging environment that exactly mirrors the production environment to allow testing of systems and applications. There is a risk that data used during testing may not be protected, leading to the risk of a privacy breach. CFPB mitigated this risk by conducting a security and privacy risk assessment on the staging environment to assess that security and privacy controls are in place prior to the use of the staging environment. In addition, data used during testing within the staging environment is not used for operational purposes. Live data is only used when systems and applications are placed into production. CFPB assessed the

privacy controls in place for all systems and applications prior to the use of live data, and appropriate PIAs and SORNs are completed to address specific collections and uses of PII.

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

AWS provides capabilities that offer CFPB ways to use and share data, such as tools that perform advanced analytics on existing data, and dynamic access controls that allow employees to share large collections of information seamlessly within the environment. Data is housed within databases and data warehouses that support AWS Alto operations and the systems and applications hosted within the environment. There is a privacy risk that PII may be used or shared for purposes other than as described within CFPB Privacy Notices, Privacy Act Statements, PIAs, and SORNs, or as authorized by law. CFPB mitigates this risk by selecting granular access controls that provide access to authorized users to data sets to safeguard the data it collects. Role-based training is also provided for the handling of PII, regardless of where this data resides within CFPB. CFPB conducts continuous monitoring of systems and PII collections to ensure that PII is being used in the manner consistent with these notices.

Data within AWS Alto may also be shared with other CFPB cloud environments for data storage purposes. For example, CFPB's Salesforce environment may collect data and then use AWS Alto to parse and organize the data prior to its use. This presents a privacy risk that PII collected within another cloud environment may be sent to AWS Alto and used by an unauthorized individual, or that a breach within the cloud environment may impact business operations within AWS Alto. CFPB mitigates this risk by sharing AWS Alto data only with systems and applications that have achieved an Authority to Operate (ATO) based upon CFPB A&A processes. Connections between other cloud environments are assessed by 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 AWS Alto.

- **Security**

Given the type and sensitivity of the information held within AWS Alto, the environment may be an attractive target for unauthorized access and/or insider threats. Data within the environment is therefore subject to the appropriate technical, physical, and administrative controls, or safeguards, as prescribed by federal security and privacy guidelines (e.g., Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) Special Publications, and CFPB policies and procedures. Specifically, for the AWS environment, CFPB has identified and implemented appropriate security and privacy safeguards (e.g.,

restricting access to only authorized users, encrypting data) to reduce the overall risk, as described further in the PIA.

Given the dynamic nature of applications and services (e.g., upgrades) CFPB has instituted a risk management process, in accordance with NIST guidance, which continuously monitors environments to determine the effectiveness of implemented controls. CFPB's risk management process identifies risk, analyzes the risk, prioritizes the risk, develops a plan to remediate the risk, and implements corrective actions/security controls to ensure that the AWS environment operates securely. CFPB ensures that the PII used within the environment is done in accordance with the applicable PIAs and SORNs. Any changes within the AWS Alto environment are also reviewed by the CFPB CCB, where CFPB architects and application developers ensure that AWS Alto product releases are coordinated and that upgrades do not affect the performance and security and privacy of applications or data within the AWS Alto environment.

To support this assessment, the CFPB Privacy team is part of governance and project working groups to assess privacy implications of systems and applications that are migrated into and developed within the AWS Alto environment.

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.

AWS Alto provides GSS services for many CFPB business functions throughout the organization. Information collected by systems and applications within Alto include the PII of members of the public and CFPB staff (e.g., employees, contractors, interns, detailees, and volunteers); financial data of entities regulated by CFPB; and contact information of individuals participating in legal matters such as judges, opposing counsel, expert witnesses, arbitrators, mediators. As the primary hosting environment for the majority of CFPB systems and applications, AWS Alto is the platform used to host the collection, storage, and processing of PII for several CFPB programs, but does not itself directly collect any PII for a specific business purpose. PII that is collected, used, and

stored by hosted systems and applications within AWS Alto varies depending on the program, but may include:

- First and last name;
- Address (business or personal);
- Phone number (business or personal);
- E-mail address (business or personal);
- Social security numbers of Bureau staff for human resource purposes;
- Financial account numbers;
- Date of birth;
- Driver's license number;
- Demographic information;
- Personal income information;
- Background check or employment related information;
- Credit card and other personal financial information;
- Employment information;
- Security logs; and
- Administrative human resource data.

Common sources of PII include, but are not limited to:

- Employees and contractors for personnel and clearance information;
- Consumers for purposes such as resolving complaints with Bureau covered entities;
- Financial institutions, data brokers, or others for market research, supervisory or enforcement activities;
- Individuals or organizations who are interested in receiving information from the Bureau on a one-time or ongoing basis;
- Member of the public submitting formal public comments on Bureau-published notices or rulemaking;
- Service providers of financial education and assistance working with the Bureau on educational projects;
- Representatives of community organizations, employers, social workers, teachers, or others who interact with consumers;

- Representatives of industry, including representatives of Bureau covered entities, State and Federal government representatives;
- Individuals who apply to serve on CFPB sponsored or affiliated advisory boards or Councils; and,
- Individuals who correspond with CFPB through routine business communications such as day-to-day email and website communications and work documents to support business functions.

AWS Alto provides numerous ways for CFPB to collect PII. For example, AWS Alto enables CFPB to create and use electronic forms or web-based forms to collect PII from consumers and financial institutions and securely upload forms to the Bureau. AWS Alto also provides CFPB access to AWS Marketplace that provides access to AWS-approved third party services that CFPB can select and use within the AWS Alto. CFPB assesses program-specific collections of data to ensure the Bureau has the appropriate legal authority to collect the data, and that only the minimal amount of PII is collected.

AWS Alto provides environment tools and components that enable CFPB to implement granular control of data collection options, such as the customization of data fields to limit the amount of PII entered by individuals. Any uses of AWS Alto-provided or AWS Marketplace tools and components for the collection of PII are also documented within program PIAs.

2. Describe CFPB's objective for the information.

AWS Alto provides the ability to collect, process, and store information, including PII, to support a variety of CFPB programs and management of systems and applications within the environment. This includes general tasks such as responding to a consumer; hosting of the CFPB public website; supporting the supervision, enforcement, investigation, and litigation processes of the Bureau; conducting consumer or market research; provisioning access to systems and applications; and related routine business communications such as day-to-day email communications. When a program needs to collect PII, CFPB assesses the design and purpose of the system or application and its use of AWS Alto as a host to collect, use and store PII. This assessment is completed by a review of system design documentation reviews and PIAs to determine whether CFPB has an authorized purpose to collect and use the information, and to ensure that PII used is both relevant and necessary to the purpose for which it is collected. Each program-specific use of PII collected by systems and applications hosted by AWS Alto is also

assessed to determine the privacy impacts, and resulting risks and mitigations are documented within 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.

AWS Alto provides a general support environment to develop applications that collect, use, maintain, and share information depending on the business need and legal authority. Generally, 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 response to a request from Congress; for a security incident involving information collected within AWS Alto; or through investigative or legal processes as part of litigation activities. When external users are provided access to an application within AWS Alto, 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 AWS Alto to other CFPB-authorized GSS cloud environments such as Salesforce 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 a risk to either environment or to the data that resides within the GSS environments.

CFPB only shares information in accordance with the business need and legal authority. CFPB documents the routine uses of information sharing with SORNs, Privacy Act Statements, and within application-specific PIAs[4].

4. Describe what opportunities, if any, individuals to whom the information pertains must (a) receive notice regarding the CFPB's

[4] Please see www.consumerfinance.gov/privacy.

use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

CFPB may collect PII directly from individuals within hosted systems and applications in AWS Alto (e.g., consumer complaints, contact requests, employment applications, Freedom of Information Act (FOIA), and Privacy Act requests). There are instances where CFPB may indirectly collection information from individuals (e.g., data from financial institutions, data brokers, or other agencies used for market research or supervision purposes, or data collected for enforcement purposes) which may be used by systems and applications within AWS Alto to analyze, organize, or store the data. When PII is collected directly from individuals, they are typically given notice of the uses and the opportunity to opt in and consent to uses. CFPB publishes PIAs and SORNs (if applicable) that provide information on how to request access or amend information in accordance with the Privacy Act and CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq. Individuals may sometimes be able to update their information directly – for example, by contacting the CFPB program directly to update contact or mailing information, or updating the 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.

CFPB conducts a full security review of AWS Alto on all applicable federal laws, directives, and standards. In addition, CFPB developed and followed a Security Implementation Plan (SIP) identifying the necessary procedures to use PII within each hosted system and application developed within the environment, with AWS Alto obtaining an ATO for its staging and production environments to securely provide the hosting environment.

CFPB issues authorized personnel access to AWS Alto following CFPB's Privileged 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 the AWS Alto, or within any of the applications within the environment. Users must also complete 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 AWS Alto environment to ensure the application design aligns with CFPB's authority to collect, use, maintain, and share PII. Privacy reviews are part of each application design, and part of any changes, modifications, or upgrades to AWS Alto.

CFPB's ability to use AWS Alto depends on implementing appropriate security and privacy controls tested and continuously monitored as part of the agency's information security and privacy programs. CFPB requires all the capabilities in AWS Alto are FedRAMP Moderate accredited and leverages the FedRAMP security assessment package. In addition, these services are subject to FISMA, federal guidance (e.g., NIST, Office of Management and Budget (OMB)), and CFPB policies and procedures.

AWS provides a GSS environment for IT solutions and functionality by providing secure workspaces that offer extensive options for configuring workflows, databases, forms, dashboards and reports, process modeling, and customizable user interfaces. AWS Alto system and application configurations can occur without any hardware or software requirements. The unique capabilities AWS provides require consistent risk management and continuous monitoring processes which are subject to and maintained by CFPB's Security and Privacy Continuous Monitoring Strategies, allowing for consistent, substantive reviews of security and privacy controls to ensure their effectiveness in adequately protecting the environment and the data residing within it.

CFPB develops systems and applications within AWS Alto 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.

In conjunction with developing this PIA, AWS Alto has been assessed to determine how its tools, components, and applications provide a more secure, automated approach for hosted business systems and applications. As a result, the following technical and administrative controls are in place to secure data and ensure accountability for CFPB's appropriate collection, use, disclosure, and retention of the information have been identified:

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to the AWS environment and to the data that resides within its applications.
- CFPB general privacy and role-based training are required prior to granting access to AWS Alto and its systems and applications within the environment. Role-based training includes data handling procedures, incident, and breach response procedures, and 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 AWS environment.

- Compliance with CFPB's cybersecurity policies and procedures are documented within the SIPs.
- CFPB assigns and maintains roles and permissions within AWS Alto and its systems and applications for each of these groups of users (employee, contractor, detailee, interns, volunteers, etc.) based on their role within the organization and as approved by Cybersecurity. The following lists examples of the roles and responsibilities within the environment:
    - 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 AWS Alto, including management of user account privileges and permissions.
    - CFPB Basic User roles - This role is assigned to all CFPB employees and contractors who are granted access to application(s) in AWS Alto. Permissions are based upon assigned business function (e.g., Contracting Office Representative (COR), Investigator, Stakeholder Support, Human Resource representative, personnel security, etc.) and security configurations are based on their business and security needs within a specific system or 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 throughout the environment.
- Security logging and monitoring tools to ensure authorized access to both the environment and to monitor system access within the environment.
- Records Schedules submitted to and approved by National Archives and Records Administration (NARA) are in place for each data collection at the system and application level. Applications that collect, use, maintain, and/or share PII may retain records indefinitely until the NARA approves CFPB's records disposition schedule. Records that fall under a general records schedule are maintained and disposed of according to the schedule identified within system/application level PIAs and SORNs for systems and applications within AWS Alto.
- Personnel Security, including background checks, are completed for all employees, contractors, or other individuals authorized to conduct CFPB activities within AWS Alto.

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 the same controls. Contractors with access to direct identifying PII within hosted systems and applications are required to report suspected or confirmed privacy incidents to 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 privacy requirements found within 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.)

AWS Alto provides CFPB with the ability to connect third-party vendor services to the environment to support enhanced performance, increased security, data storage needs, and data analytics and visualization capabilities from its Marketplace and from other CFPB cloud environments. These third-party vendors are vetted by AWS through its partnership program, and are further assessed by CFPB prior to deployment within the AWS Alto. For example, CFPB leverages tools and services within the AWS Alto to host CFPB's data, providing CFPB data scientists, data engineers and data analysts with a collaborative environment to run interactive and scheduled data analysis workloads. CFPB also connects AWS Alto with other cloud services and tools, such as Salesforce, to leverage AWS tools and components such as data storage, data analytics, etc.

Any hosted systems or applications that support or are developed within AWS Alto are managed through a project governance lifecycle where the scope and design of the system or application is assessed by CFPB's security and privacy teams to ensure compliance with CFPB policies and procedures, to include any tools and components selected from AWS Alto. AWS Alto connections with other third party cloud services, such as Salesforce and Microsoft O365, are also reviewed to ensure compliance. In addition to CFPB vetting applications and validating security controls, AWS Alto provides additional verification for applications prior to admittance to the environment. Typically, third party tools and services providers must also be assessed to identify the necessary security and privacy controls that must be implemented and achieving a separate authorization (e.g., ATO) prior to connection or support capability for AWS Alto. Depending on the connection, typical controls include:

- Memoranda of Understanding, information sharing agreements, and authority to use decisions which describe the type of data, collection method(s), use, maintenance, and sharing of any PII collected and used by systems and applications hosted within AWS Alto
- Role-based access controls within the AWS Alto environment and the systems and applications that reside within the environment
- Documented compliance with CFPB cybersecurity policies and procedures (e.g., ATO)
- Audit logs and standard operating procedures for monitoring access and activity of hosted systems and applications.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2022.12.15 11:42:36 -05'00'

Christopher Chilbert

Chief Information Officer

Date

Kathryn Fong

Digitally signed by Kathryn Fong
Date: 2022.12.15 11:51:43 -05'00'

Kathryn Fong

Chief Privacy Officer (Acting)

Date

Vivienne Gilmore

Digitally signed by Vivienne Gilmore
Date: 2022.12.14 15:59:42 -05'00'

Vivienne Gilmore

Initiative Owner

Date