Cloud 2 General Support System

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Process specific data required to carry out the various missions and operational activities of the CFPB.
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.

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act ("Act"), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau ("CFPB" or "Bureau"). The CFPB administers, enforces, and implements federal consumer financial protection laws, and, among other powers, has the authority to protect consumers from unfair, deceptive, and abusive acts and practices when obtaining consumer financial products or services.

In pursuing its mission the CFPB uses cloud-based storage and data process capabilities to support employees, contractors, partners, and the public. This cloud environment, called Cloud 2, which utilizes Infrastructure as a Service (IaaS), is a general support system ("GSS") providing a secure and scalable virtual environment for the Bureau. Specifically, the Cloud 2 provides a platform to build developmental and external facing applications and systems to support the CFPB mission.

Cloud 2 GSS provides external and internal services for the Bureau. External services consist of such things as supplying the Bureau's public facing website, the Home Mortgage Disclosure Act (HMDA) Data, and it provides access to the Extranet used for such things as secure data transfers from third party financial institutions to CFPB. Cloud 2 also provides internal services which include security defense, audit logging, data processing and integrity checks, administrative backups, and temporary storage and virus scan of data files prior to transfer.

The information that is contained or processed in Cloud 2 includes information that supports the above external and internal services. Personally Identifiable Information ("PII") may be collected from employees, contractors, consumers, individuals who work for supervised entities, and the public. The information collected could range from PII of low sensitivity such as the type of contact information found on business cards (e.g., name, email, address, and phone number) to highly sensitive information such as individuals' financial information including Social Security numbers, financial account numbers, photos, and information on the Internet Protocol (IP) address of the computer being used.

The Cloud 2 GSS PIA is meant to cover all of these types of information that are stored or processed in Cloud 2. In some cases the systems and information covered by this PIA are also covered in other PIAs, such as the GSS Infrastructure PIA, the Extranet PIA, and the Consumer Response PIA. This separate PIA is intended to discuss the distinct risk profile for these systems and data for this cloud environment. For additional information and analysis related to specific

systems, applications, and data collections, program-specific privacy impact assessments are available at www.consumerfinance.gov/privacy.

The establishment of the Cloud 2 GSS is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. Information in the Cloud 2 GSS is collected in accordance with and is compliant with applicable federal laws, including the Dodd-Frank Act, the Paperwork Reduction Act, the Right to Financial Privacy Act, and the Privacy Act of 1974.[1]

Much of the information in the Cloud 2 GSS does not constitute a system of records because it is not retrieved or retrievable by personal identifier. However, where it does constitute a system of records, the information is addressed in one or more of the Bureau's System of Records Notices ("SORNs"). A complete and up-to-date list of applicable SORNs can be found at www.consumerfinance.gov/privacy. In addition, where required by the Paperwork Reduction Act, the CFPB has received OMB approval for its information collections. For more information, see Office of Information and Regulatory Affairs Website at www.reginfo.gov.

Privacy Risk Analysis

The primary privacy risks associated with data covered by the Cloud 2 GSS PIA are risks related to:

- Confidentiality,
- Data Quality and Integrity, and
- Data Minimization.

Confidentiality: The greatest privacy concern with a cloud environment is the potential threat to confidentiality of the information contained in the cloud. However, the Cloud 2 environment has gone through a rigorous security evaluation and it is FedRAMP compliant. In addition it has been separately evaluated to ensure that it has sufficient security controls by the Bureau. While there is no way to perfectly protect any system that directly connects to the public, Cloud 2 has a sophisticated layered set of protections that minimizes the risk to data.

[1] The authorities for specific information collections are addressed in applicable System of Records Notices and program-specific privacy impact assessments, available at www.consumerfinance.gov/privacy.

Data Quality and Integrity: The Bureau collects a significant amount of information and could on occasion obtain out-of-date or incorrect information. Because the interactions that result in information collection are often voluntary and because the Bureau does not use any information collected through these types of interactions to provide or deprive an individual of a right or benefit, the privacy risks associated with these collections are minimal. While the Bureau may obtain PII from third-party sources it may be limited to that which is otherwise publicly available. In cases where information is obtained from non-public sources, the Bureau collects such information in accordance with applicable law and pursuant to applicable agreements governing the sharing of such information (e.g. Memoranda of Understanding, Memoranda of Agreement). Finally, to minimize any residual impact on individuals, the CFPB has implemented appropriate technical, physical, and administrative controls relative to the risks presented to confidentiality, information quality, and information uses. These controls are discussed in more detail in the subsequent sections of this PIA.

Data Minimization: The Bureau reviews all collections of data in an effort to try to minimize the amount of directly identifying PII to the greatest extent possible, while still allowing the Bureau to complete its objectives. This may be done by stripping collections of direct identifying PII, aggregating data, or other means of minimizing such collection. Nevertheless, the Bureau necessarily collects a significant amount of PII and consequently utilizes appropriate technical, physical, and administrative controls relative to the risk of the data. These controls are discussed below and in the appropriate PIA and SORN associated with the particular collection.

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 Cloud 2 collects, temporarily stores, and transmits PII from the external facing website (consumerfinance.gov). The CFPB limits the intake of PII to only data that is necessary for the purpose of its collection. PII could include:

- Name,
- Address (business or personal),
- Phone number (business or personal),
- E-Mail address (business or personal),

- Social Security number,
- Financial account numbers,
- Birth date or place,
- Demographic information,
- Income information,
- Employment information,
- Information from covered institutions collected for supervisory or enforcement activities,
- Information collected to support market analysis,
- Information collected to support the Bureau's educational programs, and
- Security logs.

The information may be collected directly from individuals, when possible and appropriate, or it may be collected from third-party partners, Bureau-covered entities, public sources, and others. Mostly commonly information is collected from:

- Employees and contractors for personnel and clearance information,
- Consumers in order to resolve complaints with Bureau covered entities,
- Financial institutions, data brokers, or others for market analysis, 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 education 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
- Other individuals, who interact with, or whose activities pertain to the mission of the CFPB.

In cases where the information is derived from non-public sources, such as other Federal agencies or data brokers, the Bureau obtains such information using contracts, information sharing agreements, or other similar agreements or processes, and in accordance with applicable law.

For additional information and analysis related to specific systems, applications, and data collections, program-specific privacy impact assessments are available at www.consumerfinance.gov/privacy.

2. Describe CFPB's objective for the information.

The information contained in the Cloud 2 GSS and covered by this PIA includes a variety of data. It is the primary location for HMDA data, the Consumer Response customer portal, security data, such as the audit log and other administrative data, and it temporarily stores information prior to transfer to the external party. The objectives for specific collections of information are described in the Bureau's SORNs and program-specific privacy impact assessments, available at www.consumerfinance.gov/privacy.

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

One of the primary purposes of Cloud 2 is for the Bureau to share information with the public, whether that be general information about the Bureau itself, or more specific information about a program such as HMDA, eRegs, or one of CFPB's many financial educational programs. Some of this information includes PII that has been de-identified, as is the case with HMDA data. At other times PII is shared when consent is given, as might be the case in a blog or news posting.

In addition, the Bureau may share information when working with other Federal or state governmental agencies in supervising Dodd-Frank covered entities or for purposes of enforcing various related laws or regulations. The CFPB shares information with covered entities to respond to consumer complaints. The Bureau also shares employee information with other Federal agencies and companies to support the provision of employees' salaries and benefits.

Where applicable, the CFPB may share information as outlined in the Routine Uses of the relevant SORNs and as described in program-specific privacy impact assessments, 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.

Cloud 2 contains both information that is collected directly from individuals (e.g., consumer complaints, requests to be contacted for particular purposes, employment applications, FOIA

and Privacy Act requests), and information that is not collected directly from individuals (e.g., information collected from covered entities through the Extranet). Where information is collected through the Bureau website, individuals only provide information voluntarily, with notice, and they may retract consent at any time. For further information, see the ConsumerFinance.gov privacy policy at www.consumerfinance.gov/privacy-policy.

When information is collected directly from individuals, they are given notice of the uses and the opportunity to consent to particular uses; when individuals do not consent to a particular use, the information will not be collected. Typically, individuals have opportunities to change or update information that is erroneous, out of date, or no longer relevant. Notice to individuals may be provided in the form of a Privacy Act Statement (when required by the Privacy Act of 1974), a privacy notice (when the Privacy Act of 1974 does not apply), or other methods such as an informed consent form, or instructions directing individuals to the privacy policy of a third-party partner or vendor, or to the Bureau's own privacy policy for its website, consumerfinance.gov.

Finally, the Bureau has published this and other PIAs and relies on a SORN (if applicable) and approval from the Office of Management and Budget of information collections under the PRA (if applicable) to provide notice to impacted individuals.

Where applicable, individuals may request access to or amendment of their information in accordance with the Privacy Act and the CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 *et seq*. Individuals may sometimes be able to directly update their information – for example, by contacting the Bureau directly to update contact or mailing information, or updating information provided for registration purposes for a Bureau-sponsored event.

For additional information and analysis related to specific systems, applications, and data collections, applicable SORNs and program-specific privacy impact assessments are available at www.consumerfinance.gov/privacy.

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 complies with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002; adopts Office of Management and Budget privacy-related guidance as

best practice;[2] and applies National Institute of Standards and Technology risk management processes for privacy.

The CFPB uses the following technical and administrative controls to secure the information and create accountability for the Bureau's appropriate collection, use, disclosure, and retention of the information:

- Audit Logs and Reviews,
- CFPB Personnel Privacy Training, including annual and role-based training,
- CFPB Privacy Incident Response and Recovery Plan and contractual obligations for third parties to support CFPB Privacy Incident Response and Recovery Plan,
- Compliance with CFPB cybersecurity policy and procedures,
- Information Quality and Integrity Checks,
- Extract logging and 90-day reviews,
- Policy and Standard Operating Procedures,
- Role-based Access Controls,
- Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies,
- Records Schedule Submitted to/Approved by National Archives and Records Administration (NARA): Records will be disposed of according to the applicable records schedule. Information in the Infrastructure GSS is covered by CFPB specific records schedules as well as general records schedules. Some records schedules are awaiting NARA approval, and
- Personnel Security supported through due diligence screening.

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.

[2] Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with Office of Management and Budget (OMB)-issued privacy guidance, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

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.)

The Bureau may at times collaborate with third parties. For example, CFPB may partner with other Federal, state, or local government agencies in supervisory and enforcement activities; it may work with companies about whom consumers have filed complaints; or it may share information with groups, individuals, and organizations that assist the Bureau in market analysis and development of consumer financial tools.

In all of these instances, controls are put in place to protect against inappropriate collection, use, disclosure, and retention depending on the type of sharing or data involved. Depending on the particular sharing typical controls might include:

- Compliance with CFPB cybersecurity policy and procedures,
- Data Quality and Integrity Checks,
- Extract logging and 90-day reviews,
- Policy and Standard Operating Procedures, and
- Role-based Access Controls.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2021.07.22 17:48:09 -04'00'

Chris Chilbert

Chief Information Officer

Date: 7/21/2021

TANNAZ HADDADI

Digitally signed by TANNAZ HADDADI
Date: 2021.07.23 09:02:50 -04'00'

Tannaz Haddadi

Chief Privacy Officer

Date: 7/21/2021

Vivienne Gilmore

Digitally signed by Vivienne Gilmore
Date: 2021.07.22 17:02:22 -04'00'

Vivienne Gilmore

System Owner

Date: 7/21/2021

Change control

Version	Summary of material changes	Pages affected	Date of change
7/21/2021	Re-published with updated signatories.	10	7/21/2021