Infrastructure General Support System (GSS)

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Store and transmit all 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.

cfpb Consumer Financial Protection Bureau

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 a networked infrastructure to provide the data processing and information technology (IT) connectivity needs to its employees, contractors, and partners. This infrastructure includes both hardware and software to support both mission and daily operations. As a general support system (GSS) (referred here in as the Infrastructure GSS) the environment stores and connects to other CFPB GSSs such as cloud environments, and employs major and minor applications such as firewalls, routers, and servers to provide network connectively, communications, data transfer capability, data storage, and provides tools and applications that secure these processes.

The Infrastructure GSS collects and maintains every type of information that the Bureau uses in support of its various missions, such as market data for research purposes, investigatory data for enforcement purposes, consumer complaint data for consumer response purposes, supervisory data for supervision purposes, human resources data for personnel purposes, and other types of data required for meeting operations and mission objectives. This data contains personally identifiable information (PII) of individuals who may interact or have business with the Bureau, including employees, contractors, consumers, individuals from state and federal level entities, stakeholders from industry, and individuals who work for financial institutions. This PII may range from basic contact information (e.g., name, email, address, and phone number) to sensitive information such as an individual's financial information and financial account numbers collected in support of the CFPB mission.

The Infrastructure GSS Privacy Impact Assessment (PIA) is meant to cover all types of information stored upon or that traverses the environment. The PIA is being updated to address the applications and functions the environment currently provides, and to remove references to capabilities such as identity, credentialing, and access management (ICAM) which will be assessed in a separate PIA. 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 main components, including tools and applications, of the infrastructure include:

- Client devices (e.g., laptops, smartphones)
- Physical and Virtual Servers
- Wide Area Network (WAN)
- Local Area Networks (LANs)
- Virtual networks
- Network perimeter devices and boundary protections
- Remote access devices
- Active directory
- File and print servers
- Database management systems.

The components of the Infrastructure GSS make up the fundamental hardware and software and provide connectivity, security, storage, and data access for Bureau employees and contractors. These services range from client devices where employees and contractors can do daily work to central data storage and management devices. Many of the components of the Infrastructure GSS are the physical tools or systems used to implement the security controls: access control tools and applications that provide a mechanism for moderating access requests to information, laptops, mobile devices, and other IT devices to provide network access to a distributed workforce, and network boundary protection devices to protect internal systems from unauthorized access.

The establishment of the Infrastructure GSS is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. Information in the Infrastructure GSS is collected in accordance with and is compliant with applicable federal laws, including the Dodd-Frank Act, the Paperwork Reduction Act (PRA), the Right to Financial Privacy Act, and the Privacy Act of 1974. Much of the information in the Infrastructure GSS does not constitute a system of records because it is not retrieved or retrievable by personal identifier. However, where the Infrastructure GSS is leveraged to support the uses of a system of records, the information is addressed in one or more of the Bureau's program-specific System of Records Notices (SORNs). In addition, where required by the PRA, 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 and consumerfinance.gov/privacy.

Privacy Risk Analysis

The primary privacy risks associated with data covered by the Infrastructure GSS PIA are risks

related to:

- Purpose of Collection
- Confidentiality
- Data Quality and Integrity
- Data Minimization
- Security.

Purpose of Collection

Because the information included in the Infrastructure GSS covers all the information that is collected and used by the Bureau, there is a privacy risk that the information may be used by unauthorized users or for unauthorized purposes. The CFPB mitigates this risk by ensuring that the collections and uses of all data are reviewed and that the data is only collected and used for appropriate purposes. Several of the components of the Infrastructure GSS are governed by policies and procedures that place limitations on collection and use capabilities of the information stored within the environment. For example, data may be contained in an access-controlled file system that is governed by an access management policy that is monitored by the system owner. There are also administrative procedures requiring new collections or new uses of existing data to be reviewed to ensure that they fall within existing, approved frameworks for the collection and use of data with the environment.

Confidentiality

Because information of all types, including PII, is either stored on or traverses the Infrastructure GSS, it is important that the controls exist to protect the confidentiality of the information. In the event of a breach of confidentiality, there is a risk of embarrassment or loss of reputation to both individuals and CFPB, or consumers suffering financial harm or even identity theft. CFPB minimizes this risk by enforcing access controls to minimize the number of individuals who have access to the data and by storing data on systems within the environment that have a CFPB security and privacy authorization. Further, access to information within the Infrastructure GSS must be approved through a privileged user access request which is reviewed and approved by the system owner prior to the access being granted.

Data Quality and Integrity

The Bureau collects a significant amount of information and there is a privacy risk that the Bureau could on occasion obtain out-of-date or incorrect information. However, 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 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 is often 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 Infrastructure GSS provides IT support and services to several CFPB operations, but the environment does not itself conduct direct collection of information that is stored, processed, or transmitted through the environment. This presents a risk that larger amounts of information may be collected and stored within the Infrastructure GSS than is necessary to support operations. CFPB minimizes this risk through data governance processes where information transmitted or stored by a system leveraging the GSS Infrastructure is reviewed to minimize the collection of PII to the greatest extent possible, while still allowing the CFPB to complete its business objectives. This may be achieved by stripping collections of PII to the minimum necessary, 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. Specific data minimization controls are discussed in the appropriate PIA and SORN associated with the collection of PII[1].

Security

Given the type and sensitivity of the information transmitted and stored within the GSS Infrastructure, the environment may be an attractive target for unauthorized access and/or insider threats. PII 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). CFPB has identified and implemented appropriate security and privacy safeguards (e.g., restricting access to only authorized users, encrypting data, and providing access to systems and data through system owner) to reduce the overall risk to PII within the environment.

[1] The authorities for specific information collections are addressed in applicable PIAs and SORNs available at www.consumerfinance.gov/privacy.

CFPB applies a rigorous 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 Amazon Web Services (AWS) environment operates securely. CFPB ensures that systems that transmit and store PII within the environment operate in accordance with the applicable system specific PIAs and SORNs. Any changes within the Infrastructure GSS environment are also reviewed by the CFPB change control board (CCB), where CFPB architects and application developers ensure that systems and applications within the environment do not affect the security and privacy of PII. To support this assessment, the CFPB Privacy team is part of governance and project working groups to assess privacy implications of systems and applications within the GSS Infrastructure environment.

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

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 information that is stored on or traverses the Infrastructure GSS supports all operations and mission objectives. System owners leverage the GSS Infrastructure's capabilities to transmit, store, and share PII. The specific types and amount of PII may vary depending on the nature of its use and by system. Specific system uses of PII that leverage the GSS Infrastructure are further assessed in system-specific privacy impact assessments[2]. The types of PII transmitted or stored by the Infrastructure GSS may include:

- First and last name;
- Address (business or personal);
- Phone number (business or personal);
- E-Mail address (business or personal);

[2] CFPB PIAs can be found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/

- Information provided by consumers when submitting a complaint, to include financial account numbers, or Social Security Number (SSN);
- Birth date or place;
- Demographic information;
- Income information;
- Employment information;
- Information from covered entities collected for supervisory or enforcement activities;
- Information collected to support market analysis; or
- Information collected to support the CFPB's educational, outreach, or research programs.

The Infrastructure GSS may provide support for systems to collect PII directly from individuals, third-party partners, Bureau-covered entities, public sources, and others. Common sources of PII collection may include:

- Employees and contractors for personnel and clearance information;
- Consumers 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;
- Members of the public who submit formal public comments on rulemakings;
- Financial education and financial assistance providers that work 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; or
- Other individuals who interact with, or whose activities pertain to the mission of, the CFPB.

The collection and intended use of PII supported by this environment must first be reviewed and approved by the CFPB through data governance processes. This review ensures that proposed collections of PII is the minimum necessary for the intended purpose and the authorization to do so under CFPB's regulations prior to any collection of use of PII that is housed within this

environment.

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 Infrastructure GSS is used to provide IT network capabilities for all CFPB mission and operation objectives, including the CFPB's enforcement, supervision, consumer response, market research, consumer education, and internal operations programs. The Infrastructure GSS offers a hosted environment for CFPB to design, build, and maintain systems and applications that may collect, use, share, and store PII. The objectives for specific collections of information and the uses and disclosures of PII are described in CFPB's system specific PIAs and in CFPB's SORNs, which address how each system leverages the environment to support the collection, use, storage, and disclosure of PII and the associated risks. In general, PII housed within this environment can only be used or disclosed by individuals who are authorized and approved to access this data to perform specific functions as approved by CFPB System Owners. System Owners who collect and use data within this environment are subject to CFPB's Data Governance Board processes. These processes review all proposed uses of PII to ensure that data collected is relevant and necessary for the purposed collection and use. Use and disclosure of PII is limited to the authorized uses and compatible purposes addresses in the program specific PIAs and SORNs.

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.

The CFPB shares information that is transmitted or stored on the Infrastructure GSS for various purposes. The extent of information shared, with whom the information is shared, and the method of sharing varies based on the specific mission or operational use and documented within system specific PIAs. For example, a system my use the GSS Infrastructure to transmit information through its network 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 may also use the GSS Infrastructure to share stored information related to human resource PII, such as details about employees' salaries and benefits, with the Office of Personal Management (OPM).

Where applicable, the CFPB may share information as described in the routine uses of the relevant SORNs and 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.

Some information that is transmitted or is stored within Infrastructure GSS environment is collected directly from individuals (e.g., consumer complaints, requests to be contacted for purposes, employment applications, FOIA and Privacy Act requests). Other information is not collected directly from individuals (e.g., data from financial institutions, data brokers or other agencies used for market research or supervision purposes, data collected for enforcement purposes). When systems leveraging the Infrastructure GSS collect PII directly from individuals, they are given notice of the uses and the opportunity to consent to uses; the information will not be collected if individuals do not consent to a particular use. These individuals typically 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, www.consumerfinance.gov. CFPB has also published PIAs and SORNs (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; and applies National Institute of Standards and Technology risk management processes for privacy[3]. 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 Breach Response and Recovery Plan and contractual obligations for third parties to support CFPB Privacy Incident Response and Recovery Plan
- Data quality and integrity checks are performed in accordance with the Bureau's Data Access Policy for any systems using data within the environment.
- Compliance with CFPB cybersecurity and privacy policy and standard operating procedures are documented within the security and privacy control implementation plans.
- Role-based access controls for assigning and maintaining roles and permissions within the environment and its applications based on an individual's role within the organization and as approved by system owners. The following lists examples of the roles and responsibilities within the Infrastructure GSS:
    - Infrastructure 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 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 systems, tools, and applications within the Infrastructure GSS. Permissions are based upon assigned business

3 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.

function as approved by a system owner, and security configurations are based on their business and security needs within a specific application.
    - Service account roles - Service account roles are specific non-system administrator user accounts assigned to authorized CFPB employees and contractors that are used for data synchronization, managing application programming interface (API) credentials, and to synchronize identity information.
    - Roles and responsibilities for access to CFPB systems require system owner approval.
- Records retention schedules submitted to and approved by National Archives and Records Administration (NARA) will be maintained and disposed of according to the applicable schedule.
- Personnel security is established and maintained to restrict access to on-premises equipment serving the GSS Infrastructure.

The CFPB uses contractors to help support the Infrastructure GSS, and they 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.

CFPB has updated this PIA as a result of its evolving uses of cloud GSS systems that replaced transitional system operations residing within the Infrastructure GSS. New cloud GSS environments and the systems that reside within them will be assessed in separate PIAs.

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.)

CFPB collaborates with third parties in several ways. 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; it may share information with groups, individuals, and organizations that assist the CFPB in market analysis and development of consumer financial tools. PII stored within the environment or transmitted through the environment to authorized third parties are approved by system owners and permitted by CFPB regulations. Third parties that collaborate or partner with CFPB must abide

by applicable contractual privacy clauses, memoranda of understanding (MOU), interconnection security agreements (ISA), or other third-party agreements that describe privacy policies and procedures for the handling of CFPB PII. Such agreements are reviewed by CFPB to identify and address privacy risk prior to engagement with third parties supporting this environment. The Infrastructure GSS also connects with third-party applications, data, and devices used by CFPB, such as AWS Alto and Microsoft O365, through integration tools like MuleSoft, which allows CFPB to create reusable network connections with application APIs and file sharing applications and tools to move information between systems and environments. These connections are secured using access controls and are reviewed and approved by system owners and CFPB's cybersecurity program.

In all these various 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 initiative, typical controls might include:

- Compliance with CFPB cybersecurity policy and procedures
- Data quality and integrity checks
- Policy and standard operating procedures
- Role-based access controls.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2023.06.14 17:13:25 -04'00'

Chris Chilbert

Chief Information Officer

Date

Kathryn Fong

Digitally signed by Kathryn Fong
Date: 2023.06.16 13:48:05 -04'00'

Kathryn Fong

Acting Chief Privacy Officer

Date

THOMAS MCCARTY

Digitally signed by THOMAS MCCARTY
Date: 2023.06.13 08:59:46 -04'00'

Tom McCarty

Initiative Owner

Date