General Support System

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.

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 nationwide, networked infrastructure to provide the data processing needs to employees, contractors, and partners. This infrastructure includes both hardware and software to support both mission and daily operations. This general support system ("GSS") contains or connects to other GSSs such as cloud environments and an Extranet, as well as major and minor applications such as the Matters Management System, and the Consumer Response System.

The information that is contained on, or is transported over, the Infrastructure GSS includes every type of information that the Bureau uses in support of its various missions, including market data for research purposes, investigatory data for enforcement purposes, consumer complaint data for consumer responses 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 at times contains Personally Identifiable Information ("PII") of employees, contractors, consumers, individuals who work for supervised entities, and others. This 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 individual's financial information including Social Security numbers and financial account numbers.

The Infrastructure GSS PIA is meant to cover all these types of information that exist on, or traverse the Bureau's technical infrastructure. 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 of the infrastructure include:

- Client devices
- Servers
- WAN
- MAN

- LANs
- Virtual Networks
- Network Perimeter Devices and Boundary Protections
- Remote Access Devices
- Active Directory
- File and Print Servers
- Database Management Systems
- Messaging Servers and Systems
- Identity, Credentialing, and Access Control Management Systems
- GitHub

The components of the Infrastructure GSS make up the fundamental hardware and software that provide connectivity, security, storage, and data access for Bureau employees and contractors. These 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 systems provide a mechanism for moderating access requests to information, remote access devices appropriately limit access to systems to a distributed workforce, boundary protection devices 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.[1]

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 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 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.

[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.

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, and
- Data Minimization.

Purpose of Collection: Because the information included in the Infrastructure GSS covers nearly all the information that is collected and used by the Bureau, it is important that the collections and uses of all data be reviewed to ensure that the data is only collected and used for appropriate purposes. A number of the components of the Infrastructure GSS place limitations on collection and use capabilities. For example, data may be contained in a role-based access controlled file system. 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.

Confidentiality: Because information of all types, including sensitive personal information, 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 the Bureau. In the case of sensitive PII, a breach of confidentiality could result in employees, contractors, or consumers suffering financial harm or even identity theft. The Bureau 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 that have been accredited as secure for this type of data. Staff are also trained on how to handle potential breaches to minimize negative impacts.

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 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 Bureau reviews collections of data in an effort to try and minimize the collection 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 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 information that resides on or traverses the Bureau infrastructure supports all operations and mission objectives. It may include either PII or non-PII as needed to support these objectives. The CFPB takes steps to limit its intake to PII 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, and
- Information collected to support the Bureau's educational programs.

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,
- Members 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 covered by this PIA is used to support all Bureau mission and operation objectives, including the Bureau's enforcement, supervision, consumer response, market research, consumer education, and operational activities. 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.

The CFPB shares information that transverses or resides on the Infrastructure GSS for a number of purposes. The extent of information shared, with whom the information is shared, and the method of sharing will vary based on the specific mission or operational use. For example, 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 such 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.

Some information that transverses or resides on the Infrastructure GSS is collected directly from individuals (e.g., consumer complaints, requests to be contacted for particular 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 information is collected directly from individuals, they are given notice of the uses and the opportunity to consent to particular 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,

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,

[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.

- 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.
- 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.

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 in a number of 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 Bureau in market analysis and development of consumer financial tools.

In all of 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 particular initiative, 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

_____

Ashwin Vasan

Chief Information Officer

Date

_____

Claire Stapleton

Chief Privacy Officer

Date

Change control

Version	Summary of material changes	Pages affected	Date of change