Extranet PIA

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Extranet Infrastructure to allow certain controlled interactions into the CFPB network.
Are there controls to enforce accountability?	Yes.
What opportunities do I have for participation?	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 (2010), 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 practices when obtaining consumer financial products or services. In order to support the Bureau's mission it requires general support systems (GSS) that serve as the IT infrastructure for the applications that collect, process, disseminate, and store information. This Privacy Impact Assessment (PIA) covers one portion of the Bureau's IT infrastructure, the Extranet 2.0.

The Extranet is a mediated network that allows external, authorized users limited access to the Bureau's internal network. The CFPB intends to use the Extranet to facilitate the transfer of data from supervised entities to the Bureau in the course of examinations. Although the Bureau's Extranet may eventually support other types of external users, the current implementation of the Extranet covered by this PIA will be limited to support of Supervision activities. Typically, the Bureau will contact the supervised entity and provide them with the credentials needed to establish a secure account for accessing the Extranet, along with a list of the documents requested, as part of the normal supervision examination process. The supervised entity POC will set up a secure account which will be confirmed by the Bureau. The POC will then upload the requested documents directly to the Bureau. This replaces the typical current process of the supervised entity sending the documents on encrypted CDs.

Where records are retrieved by personal identifier, the information may be documented in one or more System of Records Notices (SORN), including: CFPB.002 – Depository Institution Supervison Database; and CFPB.003 Non-Depository Institution Supervision Database.

This collection does not implicate the Paperwork Reduction Act.

Privacy Risk Analysis

The primary privacy risks associated with this implementation of the Extranet are risks related to:

- Data minimization, and
- Individual participation

Data Minimization: While the Extranet users will be told what information is needed to be uploaded to the Bureau, it will be up to the users to limit the data to only that data required. In responding to the Bureau's request, users could upload additional information that goes beyond the minimal required. Because the Extranet is a tool that facilitates transmission and storage of information – and not for reviewing the specific data – these risks are unchanged from the current process of transmitting the examination information on an encrypted CD. In addition, this risk is minimized because the supervised entity will likely have an interest in limiting the information to the greatest extent possible.

Individual Participation: Although typically the information submitted to the Bureau using the Extranet will contain minimal PII, those individuals to whom PII may pertain would not generally be consulted regarding the transfer of information to the Bureau in the supervisory context. This PIA and applicable Systems of Records Notices provide constructive notice about the data's transfer to the Bureau. In addition, any risks related to Individual Participation are unchanged from the current process of transmitting the examination information on an encrypted CD.

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

Privacy Risk Management

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

During the first phase of its implementation, the Extranet will be used during depository and non-depository supervisory examinations for the transfer of data from the institution to the Bureau. The Bureau will make a request to the institution for the data and will provide the credentials to access the Extranet. The institution's point-of-contact will securely log on and upload the requested data which will be securely transmitted to the Bureau. Data may include information provided by the supervised institution such as:

- Institution customer name, address, phone number, email address, account information, and date of birth,
- Institution official contact information of POC, officers, executives, auditors, and directors,
- Confidential Supervisory Information and other personally identifying information related to the examination.

The Bureau mitigates the risk of receiving more information than it needs by specifying the information it seeks in information requests. The institution, in turn, provides the information required by the request.

2. Describe CFPB's objective for the information.

In the first phase of implementation the Extranet will be used by the Bureau in order to carry out its supervisory examination responsibilities. The objective for the use of the Extranet in the data collection is to provide a faster and more secure mechanism for transmitting the data, rather than mailing hard copies or encrypted CDs.

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 data may be shared for enforcement actions, actions in Federal court, and coordination with other financial regulatory agencies. The data may be used to support investigations or be used as evidence by other supervisory or law enforcement agencies. A complete list of potential third party disclosures is described in the two SORNs that cover this PIA, CFPB.002 – Depository Institution Supervison Database; and CFPB.003 Non-Depository Institution Supervision Database.

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.

In most cases during supervisory examinations the Bureau will not have access to personally identifiable information (PII). However, to the limited extent that it does, individuals typically

do not have specific notice of the CFPB's use of the information or the ability to consent to such use. Individuals are provided with constructive notice of the Bureau's use of this information through this PIA and the SORNs CFPB.002 – Depository Institution Supervison Database; and CFPB.003 Non-Depository Institution Supervision Database.

The CFPB gives individuals the ability to request access and amendment to their personal information in accordance with the Privacy Act and the CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq.

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 Bureau complies with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002; voluntarily adopts Office of Management and Budget privacy-related guidance as best practice;[1] 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 data 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
- Compliance with CFPB cybersecurity policy and procedures
- Policy and Standard Operating Procedures
- Role-based Access Controls, including user accounts for the supervised entity POCs that provide limited access to the Extranet

[1] 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 follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

- Records Schedule Submitted to/Approved by National Archives and Records Administration: The CFPB maintains computer and paper records indefinitely until NARA approves the CFPB's records disposition schedule. The CFPB will continue to retain these records until a CFPB records schedule is approved by the National Archives and Records. Records that fall under a general records schedule will be disposed of according to the applicable schedule.
- Personnel Security including background checks.

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.)

When supervised entites interact with the Bureau using the Extranet, its use is subject to the controls used to protect against the inappropriate collection, use, disclosure, and retention of data are coved in questions one through five above..

Document control

Approval

Nellisha Ramdass

For the Chief Information Officer

November 14, 2014

Claire Stapleton

Chief Privacy Officer

November 14, 2014

Neeraj Gupta

Initiative Owner

November 14, 2014

Change control

Version	Summary of material changes	Pages affected	Date of change