MAY 22, 2012

Privacy Impact Assessment

scheduling and examination system

Contact Point:
Claire Stapleton
Chief Privacy Officer
1700 G Street, NW
Washington, DC 20552
202-435-7220
claire.stapleton@cfpb.gov

DOCUMENT PURPOSE

The Privacy Impact Assessment or "PIA" provides the public with information about the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") collection and use of personally identifiable information ("PII"). PII is any information "that can be used to distinguish or trace an individual's identity"[1] like a name, address, Social Security number, or place and date of birth. The CFPB uses PIAs to document that the PII it collects is used, secured, and destroyed in a way that protects each individual's privacy. Each PIA is broken out into sections that reflect the CFPB's Privacy Principles. The CFPB's Privacy Principles are a set of nine rules the CFPB follows when it collects or uses PII.

OVERVIEW

PROJECT / SYSTEM NAME: Scheduling and Examination System

PROJECT/SYSTEM INCLUDES INFORMATION ABOUT:

- ☒ Federal Employees
- ☒ Contractors
- ☒ Consultants
- ☒ The Public

PROJECT/SYSTEM INCLUDES:

- ☒ Name and other biographic information (e.g. date of birth)
- ☒ Contact Information (address, zip code, telephone number, email address)
- ☒ Social Security number ("SSN") or other identifier
- ☒ Financial Information
- ☐ User and Online Information
- ☒ Third Party Information
- ☐ Other Information (including biometric information and health or medical information)

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

One of the CFPB's primary responsibilities is to supervise companies that provide consumers with financial products or services, such as loans or deposit accounts. For the purposes of this PIA, "companies" includes all entities for which the CFPB is responsible for supervision under the Act. The CFPB has supervisory authority over more than 100 depository companies with

[1] Office of Management and Budget (OMB) Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, (OMB M-07-16) defines PII as information which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

over $10 billion in assets. This includes large banks, credit unions, and their affiliates. It also has authority over non-depository companies. These include mortgage companies, brokers and servicers, payday lenders, private education lenders, and others.

The CFPB supervises companies by gathering and evaluating information to determine whether the companies comply with federal consumer financial laws, pose risks to consumers and whether they have systems to maintain such compliance. If the CFPB determines that companies are not in compliance, it may require corrective actions.

The CFPB outlines its approach to supervision in its Supervision and Examination Manual. More information about the supervision process, including who the Bureau has authority over is available here.[2]

The CFPB uses the Scheduling and Examination System ("SES") to carry out its supervision activities. Specifically, the SES serves as:

- A tool for scheduling examinations;
- A document repository for storing documents related to the examination and supervision process, including examination planning documents; and
- A system for compiling and managing information related to the examination of specific companies, including the storage of rating information derived from the examination process.

Through the SES, the CFPB collects and maintains a variety of PII, including PII about consumers who are past, present, or potential customers of depository and non-depository companies under the authority of the CFPB, PII about company employees, and PII about CFPB employees who are involved in the supervision process. The ways in which the CFPB collects, maintains, and uses PII in the SES is documented in two (2) separate System of Records Notices ("SORNs"), CFPB.002 –Depository Institution Supervision Database [76 FR 45766], and CFPB.003 – Non-Depository Institution Supervision Database [76 FR 45766].

[2] The CFPB's Supervision and Examination Manual – Version 1.0, is available at http://www.consumerfinance.gov/guidance/supervision/manual/

SECTION 1.0 Purpose of Collection

The CFPB will state the purpose and legal authority for collecting PII.

1.1 Why is the information being collected?

The CFPB collects and maintains PII in the SES to facilitate the supervision of companies under the Bureau's authority as well as their affiliates and service providers.

1.2 What legal authority and/or agreements allow the information to be collected?

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Act), Public Law No. 111-203, Title X provides authority for the SES. Specifically, Pub. L. No. 111-203, Title X, Section 1011, 1012, 1021, 1024, 1025 and 1026, codified at 12 U.S.C. §§ 5491, 5492, 5511, 5514 5515, and 5516.

1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

Yes. Information in the SES is searchable by name (individual or company).

The SES has a search function that primarily allows for searching by company name, names of key individuals at a company, or individual name if a sole proprietorship. The system can also retrieve by CFPB employee name. The SES does not have the capability to perform a system-wide search within uploaded electronic and imaged examination documents; however, users can conduct such a search at the document level.

The CFPB System of Records Notices, CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database documents the collections of information that populate this system.

1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration ("NARA") for the information system(s)? Explain how long and for what reason the information is retained.

The CFPB maintains computer and paper records indefinitely until NARA approves the CFPB's records disposition schedule. Records that fall under a general records schedule will be disposed of according to the applicable schedule.

1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act ("PRA")?

The SES does not use a form subject to PRA requirements to collect information for the system; however, it may store documents that were subject to PRA requirements.

1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will the CFPB mitigate these risks?

There are no identifiable risks associated with the purpose of this system.

SECTION 2.0 Openness and Transparency

The CFPB will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.

2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.

When the CFPB collects PII from companies about their customers during the course of the CFPB's supervisory activities, the CFPB does not provide notice to the individual customers pursuant to an exception to the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq*. However, this PIA and the associated SORNs CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database provide constructive notice of the CFPB's information collection practices.

When the CFPB collects PII about company employees and CFPB employees who are involved in supervisory activities, it will often collect such information directly from those individuals. In instances where the CFPB does not collect information directly from the individuals, such as when it collects information from federal databases and other agencies, the CFPB may not provide the individuals with actual notice of its information collections. However, this PIA and the associated SORNs, CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database provide constructive notice of the CFPB's information collection practices.

2.2 Will individuals be given notice prior to their information being shared? If not, please explain.

In most cases, the Bureau will not provide actual notice to individuals prior to sharing SES information that pertains to them. However, the CFPB has provided constructive notice of how it will share information stored in the SES in its SORNs, CFPB.002 – Depository Institution Supervision Database, CFPB.003 – Non-Depository Supervision Database and through this PIA.

2.3 Are there any privacy risks for this system that relate to openness, and transparency? If so, how will the CFPB mitigate these risks?

No. There are no identifiable risks related to openness and transparency for this system.

SECTION 3.0 Data Minimization

The CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. The CFPB should keep PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system?

The SES contains PII about those associated with companies supervised by the CFPB, including:

- Current and former directors, officers, employees, agents, shareholders, and independent contractors of depository and non-depository companies;
- Current and former customers of depository and non-depository companies; and
- Current and former CFPB employees assigned to coordinate examinations, provide analysis, or other duties related to the supervision of these companies.

3.2 What PII will the system include?

The system contains PII regarding consumers or customers of depository and non-depository companies, as well as employees of those companies. The system also contains information about CFPB employees assigned to duties related to the supervision of these companies.

Information about customers may include:

- Names
- Account numbers
- SSN
- Addresses
- Phone numbers
- Email Addresses
- Dates of birth
- Transactional histories
- Information related to complaints they have filed with the CFPB through the Consumer Response System[3]

Information about company employees may include:

- Names

[3] For more information on the CFPB's Consumer Response System, visit www.consumerfinance.gov/privacy.

- Titles
- Addresses
- Phone numbers
- Email addresses

Information about CFPB employees may include:

- Names
- Titles and/or role within the CFPB
- Contact information such as work address, phone number and email address
- Scheduling and work flow information

3.3 Why is the collection and use of the PII necessary to the project or system?

As noted above, one of the CFPB's chief responsibilities is to supervise companies that provide consumer financial products and services. To determine whether consumer financial products and services comply with federal consumer financial laws, the CFPB communicates with company employees who are responsible for developing, selling, marketing, and administering these products and services, as well as employees generally responsible for managing the company and its legal compliance responsibilities. In the course of these communications, CFPB examiners collect PII about the employees to the extent necessary to identify them and to facilitate further communications. CFPB examiners also review individual transaction records in the course of determining whether a company is conducting its business in accordance with applicable federal laws. Those transaction records – which contain PII about customers who have been offered or who have purchased the products and services being examined – often become part of the examination "workpapers" – records that support an examiner's conclusions about a company's compliance. The records are particularly important if the conclusion is that a company has not been properly following the law, because in those instances, the CFPB may order the company to correct its mistakes. Corrective actions may require identifying customers whose accounts reflect non-compliance, and taking specific steps to remedy the non-compliance.

3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?

The system does not aggregate data nor create new data about individuals.

3.5 What controls exist to protect the consolidated data and prevent unauthorized access?

The system does not consolidate or aggregate any data, nor create new data about individuals.

3.6 Will the system monitor the public?

The system does not monitor the public.

3.7 Will the system monitor employees or contractors?

The system includes information about CFPB employees assigned tasks related to supervision This may include examination scheduling information, login and use information related to the system, and workflow information.

3.8 What kinds of reports can be produced on individuals? Will the data included in the reports produced be made anonymous?

The CFPB may generate examination reports from the SES upon conclusion of its examinations. Such reports include lists of names and contact information of company and CFPB employees. In addition, such reports may include the names and account numbers of company customers. If examiners find apparent legal violations that the company is directed to correct, reports will generally include specific transaction examples.

The Bureau distributes its exam reports internally only to employees with a bona fide need for such reports to carry out their assigned job responsibilities.

Externally, the Bureau discloses reports to a limited group of company employees who review the results of supervisory examinations and, as required or necessary, to other state and federal government agency employees whose job functions allow them to review reports generated from a CFPB examination. Section 4.2 of this PIA and the SORNs, CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database, as well as www.consumerfinance.gov/wp-content/uploads/2012/01/GC_bulletin_12-01.pdf, outline the ways the CFPB may share information from this system with other federal and state agencies.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will the CFPB mitigate these risks?

There is a risk that documents or other information provided by companies to the CFPB during the examination process could include unnecessary PII about customers or employees of the company. To help mitigate this risk, the CFPB trains examiners to collect only relevant and necessary information, as well as how to properly handle and protect sensitive, confidential, and personal information. These topics are covered in a confidentiality and privacy briefing provided when new examiners are hired. The CFPB works directly with the companies it supervises to limit the amount of sensitive information divulged during the examination process.

SECTION 4.0 Limits on Uses and Sharing of Information

The CFPB will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the collection?

Some documents provided to the CFPB by companies during the examination process could include unnecessary PII about customers or employees of the company. Section 3.9 discusses this risk and the CFPB's strategy for mitigating it.

4.2 Will the CFPB share any of the information with other individuals, federal and/or state agencies, or private sector organizations? If so, how will the CFPB share the information?

The CFPB may share PII from the SES with other federal or state government agencies to fulfill its supervisory or enforcement responsibilities. In some cases, the Dodd Frank Act requires us to share supervision and examination information with certain agencies. In other cases, we have chosen to work with related agencies, which may involve sharing information derived from the examination process. You can learn more about how we share information derived from the examination process in the CFPB Bulletin found at www.consumerfinance.gov/wp-content/uploads/2012/01/GC_bulletin_12-01.pdf.

The CFPB will only share information with authorized users through secure channels, such as encrypted email, with appropriate data sharing agreements in place.

Internally, the CFPB may share information from the SES, in the form of reports or through access to the system, with members of the enforcement, research, rulemaking, and regulations, and fair lending teams. As stated above, information access is limited based on the end users need to know the PII and job function within the CFPB.

The CFPB has outlined the ways in which information from the SES may be shared under the "Routine Uses" section of the related SORNs, CFPB.002 –Depository Institution Supervision Database and CFPB.003 – Non-Depository Institution Supervision Database.

4.3 Is the information collected directly from the individual or is it taken from another source?

A large portion of the PII the CFPB collects for the SES relates to individuals in their business or professional capacity and is collected from companies the CFPB supervises. The system also collects PII from customers of supervised companies and from consumer complaints, and from employees of the CFPB. The CFPB may also collect information from third-party sources, including other federal and state agencies with a related or similar function. Section 3 has more information about the information that is collected by the system.

4.4 Will the project interact with other systems, whether within the CFPB or outside of the CFPB? If so, how?

At this time, the SES is not capable of connecting to or interacting with other systems, either within the CFPB or outside of the CFPB. In the near future, the CFPB hopes to connect the SES to its human resources systems in a way that automates the processes of granting SES access to new CFPB examiners and tracking CFPB examiners' travel arrangements. Currently, these processes are completed manually.

4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will the CFPB mitigate these risks?

There are no risks associated with use limitation for this system.

SECTION 5.0 Data Quality and Integrity

The CFPB will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Some information in the SES is verified for accuracy and completeness as part of the supervision and examination process. The CFPB also verifies some of the information through third-party sources, including paid subscriptions or through other federal agencies.

Information about customers of supervised companies is only verified to the extent it is relevant to the examination. For example, the accuracy of a customer's information may not directly impact the outcome of an examination. The CFPB may look at whatever information the company used to make a particular decision related to a rule, regulation, or law. Other times the CFPB may need to verify customer information because it would be important to the outcome of what the CFPB is reviewing in the course of our examination of a company. The CFPB may contact customers to verify information in the course of an examination.

CFPB employees whose information (related to their job function) is contained in the system work with their supervisor to verify their own information for accuracy and completeness.

5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will the CFPB mitigate these risks?

While there is a risk that information contained in the system may be erroneous, incomplete, or outdated, the CFPB relies on information in the SES to make decisions about the companies it supervises, including demanding corrective actions, etc., and not about individuals (unless those individuals are acting as a business, e.g. a sole proprietorship). Since the CFPB would only take action against a company, and not an individual, erroneous data contained in the SES

would not result in an adverse determination or consequence for an individual and does not pose a threat to privacy.

SECTION 6.0 Security

The CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who will have access to the data in the project? What is the authorization process for access to the project?

The Bureau restricts internal access to the SES to employees who have a bona fide need for such access to carry out their assigned job responsibilities. Even then, the CFPB limits the extent of access depending upon whether employees need to see PII to perform their job responsibilities. To the extent that employees do not need to see PII, the CFPB typically provides data to these employees in a report form that is stripped of PII rather than providing them with user access to the SES.

As a general matter, the CFPB grants SES access only to authorized personnel who have been issued non-transferrable access codes and passwords and have completed appropriate training on the system, including a briefing on confidentiality and privacy. Some of the information in the SES may also be maintained in locked file cabinets or rooms with access limited to those personnel who require access as part of their official duties.

6.2 Has the CFPB completed a system security plan for the information system(s) supporting the project?

The CFPB has completed a system security plan for the General Support System ("GSS"), which the SES resides on. The system was issued an Authority to Operate ("ATO") at the Moderate level by CFPB. The ATO was signed on September 30, 2011.

6.3 How will the system be secured?

The CFPB issues authorized personnel non-transferrable access codes and passwords to the SES as required for fulfilling official duties. These codes and passwords are only issued after employees have completed the system's training seminar, which includes confidentiality and privacy briefings. Since access to all information included in the SES may not be necessary for all CFPB employees with supervision responsibilities, the system has unique user roles. For example, employees who supervise other employees with examination responsibilities may require access to human resources systems associated with scheduling, whereas employees tasked with non-examination duties may not require such access. The user roles assigned to each employee when they are granted access to the system reflect their individual needs for information in the system.

Since most CFPB examiners work remotely, they are provided identification tokens that, when combined with a selected pass code, allows them to remotely log into the CFPB's GSS through a

secure channel from their laptops. After remotely logging in, examiners may then log in to the SES using their specific credentials for the system.

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

The CFPB relies on the Treasury Department's directives related to security and privacy incidents. The CFPB is developing supplemental interim incident-reporting materials, and, upon moving onto its own network infrastructure, will issue new directives related to security and privacy incidents.

Because the SES is housed on the CFPB's GSS, the CFPB has worked closely with its selected vendor to develop an incident-reporting plan and procedures for handling a security incident involving the GSS.

6.5 Are there any privacy risks for this system that relate to security? If so, how will the CFPB mitigate these risks?

There is a risk that the large amounts of information on consumers and their financial transactions contained in the SES will attract hackers, identity thieves, and other cyber-threats. The CFPB has mitigated this risk by implementing extensive security controls and safeguards for the SES and the GSS which hosts it to protect information contained in the system against unauthorized disclosure and access.

There is also a risk that unauthorized individuals may gain access to the information in the SES. The CFPB has mitigated this risk by only granting access to the system to authorized users who, based on their need to know, will be restricted to the minimal amount of data required or appropriate to carry out their assigned job responsibilities. Access is terminated or reduced as necessary should the employee or contractor no longer have a need to know the information, change job functions, is terminated or resigns.

SECTION 7.0 Individual Participation

The CFPB will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Depository and non-depository company customers and employees do not have opportunities to opt out or decline to provide information to the SES. CFPB employees have limited opportunities to opt out if their job within the CFPB is related to examinations or supervision. Most of the data collected by the SES is provided by a company pursuant to applicable laws and regulations rather than directly from customers.

7.2 What procedures will allow individuals to access their information?

The CFPB offers a means through the Privacy Act for individuals to access, amend, or correct, their records at their request. Information about Privacy Act requests is available in the SORNs for the SES, and at www.consumerfinance.gov/foia. It is important to note that some information in the SES may not be able to be accessed or changed if doing so would impact the CFPB's ability to supervise a company or if doing so would harm a pending investigation or enforcement action.

7.3 Can individuals amend information about themselves in the system? If so, how?

The CFPB provides a means through the Privacy Act of amending or correcting your information in the SES, which is described above in Section 7.2.

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will the CFPB mitigate these risks?

There is a risk that some individuals may not have the opportunity to decline to provide information to the SES, or to update or correct information submitted.

Some of the information included in the SES cannot be accessed or amended by the public because allowing access would jeopardize a pending CFPB examination, investigation or enforcement action. This risk is acceptable because examining companies and collecting the right information in order to do so, is mandated by the Act.

SECTION 8.0 Awareness and Training

The CFPB will train all personnel about the proper treatment of PII.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

The CFPB offers privacy and security training to all employees of the CFPB, including contractors who handle PII on behalf of the CFPB.

Additionally, those with access to the SES receive training that includes a briefing on confidentiality before they are granted their access codes and passwords for the system. This briefing includes a reminder that employees accessing the system are subject to the Privacy Act.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will the CFPB mitigate these risks?

There are no risks associated with awareness and training for this system.

SECTION 9.0 Accountability and Auditing

The CFPB is accountable for complying with these principles. We will regularly check that we are meeting the requirements and take appropriate action if we are not doing so.

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

The CFPB provides its employees with appropriate privacy and security training to ensure information is used and secured appropriately. The CFPB has also implemented a rigorous set of security controls for the SES, and has limited access to those CFPB employees with a clearly defined business need to know the information. The SES does not connect to other information systems outside or inside of the CFPB.

Additionally, all CFPB systems, including the SES, are subject to periodic external audits to ensure that the CFPB protects and uses information appropriately.

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will the CFPB mitigate these risks?

The SES has limited internal auditing capability at this time, which is limited to user login, upload history and related functions. The system is not configured to audit extracts and other reports run from the system. However, the CFPB has mitigated this risk by limiting who has access to the system, clearly defining and assigning user roles with limited permissions, and providing users with training on use of the system, including privacy, security, and confidentiality.