MAY 24, 2013

Privacy Impact Assessment

LITIGATION AND INVESTIGATION SUPPORT TOOLSET

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

Consumer Financial Protection Bureau

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 how 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: Litigation and Investigation Support Toolset

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.

In carrying out its responsibilities, the CFPB will be involved in various legal issues, including conducting investigations and analysis on subjects of investigative or other interests, bringing civil and administrative law enforcement actions against companies and individuals subject to its authority, and defending itself in litigation.

To manage these functions the CFPB has created the Litigation and Investigation Support Toolset (the "LIST") which is a collection of systems and processes (components) used to

[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."

effectively collect, store, process, transmit, and maintain critical information related to investigations and litigation (potential, anticipated, pending, or closed) for the Bureau.

Attorneys, investigators, and other staff use the LIST to acquire, analyze, organize, and present large volumes of complex information and evidence. In some cases the tools facilitate the forensically sound collection of such information, or are used to process and prepare information for use in desktop-based case management tools like the Bureau's Matters Management System[2], or on the Bureau's local network. In other instances, it may allow for the ability to collect such information anonymously or through un-attributable means.

The LIST is composed of customized commercially available off-the-shelf ("COTS") computer hardware and software, and contracted staffing and related support services such as:

- Computing and networking equipment, including software, which can be used to solve unique document review and analysis issues (e.g. the review of large volumes of documents or voice recordings through internal or hosted solutions);
- Ancillary tools that support functions needed throughout the lifecycle of an investigation;
- Tools (e.g. access controlled and off-network laptops) and computer applications (e.g. for screen captures or tracing IP addresses) that allow CFPB employees to conduct research and investigations or surf the web anonymously or through un-attributable means, or to conduct other types of anonymous investigations[3] (collectively "investigation lab");
- Capabilities and tools that support background investigations, link analysis, and data analytics for research and investigatory purposes:
- An inventory of encrypted hard drives, thumb drives, and other portable media for use in transferring and/or receiving data;
- Staffing and support services related to document scanning, forensics collections, court reporting, and transcription services and;
- As necessary, access to automated litigation support ("ALS") services, which may include technical and staffing resources.

The CFPB is publishing this PIA to document its use of the LIST and its impact on privacy. In addition, the CFPB has documented in multiple CFPB System of Records Notices ("SORNs") the records about individuals collected in or processed by the LIST. Records pertaining to individuals related to investigations or litigation are accounted for in the Bureau's SORNs CFPB.004 – Enforcement Database [76 FR 45757], and CFPB.018 – Litigation Files [77 FR 27446], while records related to individual users of the LIST are accounted for in the Bureau's SORN CFPB.014 – Direct Registration and User Management System [77 FR 24185].

---

[2] The Matters Management System PIA is available at http://www.consumerfinance.gov/privacy-office/enforcement-database/

[3] As part of enforcing consumer financial laws, the Bureau is interested in understanding the types of products and services offered online through the internet or through telemarketing, in helping consumers avoid fraudulent, unfair, or deceptive practices in the online consumer financial marketplace, and in ensuring that these consumers have access to accurate information when making decisions about which product or service to select.

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, maintains, and processes PII in the LIST to support the CFPB's enforcement and litigation activities, including:

- Investigating and enforcing consumer financial protection statutes and regulations;
- Locating victims of such consumer financial protection statutes and regulations, or assisting with redress;
- Investigating internal matters; and
- Defending against suits brought against the Bureau.

The LIST also allows the Bureau to accomplish investigative and litigation tasks, including:

- Gathering and storing information in a secure and forensically sound manner, including electronic and non-electronic (e.g. paper) information;
- Gathering and storing information through un-attributable means or conducting anonymous investigations;
- Performing computer forensic analysis and processing;
- Conducting internet searches for subjects of interest;
- Analyzing, processing, formatting, and organizing electronically stored information for search, retrieval, review, correlate, flagging, and presentation;
- Processing and preparing information for use in desktop-based review or case management tools or on the Bureau's local network; and
- Assisting in the production of information captured from opposing counsel, third parties, and courts, and preparing for courtroom presentation.

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 LIST; specifically, Pub. L. No. 111-203, Title X, Section 1061, codified at 12 U.S.C. § 5581.

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. Users may search the information in the LIST by PII as part of user-generated queries. The PII by which LIST may be searched includes, but is not limited to name, address, and other identifiers. One of the primary functions of the LIST is the analysis, formatting, correlating, and organizing of investigatory information for easy search, retrieval, and review by Bureau employees, including the retrieval of data by personal identifiers.

The CFPB System of Records Notices, CFPB.004 – CFPB Enforcement Database, CFPB.018 – Litigation Files, and CFPB.014 – Direct Registration and User Management System document the collections of information that populate the LIST.

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 LIST does not use any form(s) 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 is no identified risk associated with the purpose of the collection for 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.

Wherever required, the CFPB provides notice to individuals about its policies regarding the use and disclosure of information at the time the information is collected. Given the broad collection of information from various sources in the LIST, notice may be provided in multiple formats, or in a limited format.

For information collected pursuant to a request from the CFPB, notice is provided as part of the request (e.g. in a letter request, or in the document outlining the compulsory process request).

For information that is collected via a CFPB sponsored website (like www.consumerfinance.gov) or through the Bureau's Consumer Response function, notice is provided at the point of collection through a Privacy Act statement or the Bureau's web privacy policy.

For information collected from internal CFPB systems for internal investigations or the defense of suits brought against the Bureau, staff are informed that the agency's computing systems are monitored and that personal information may be collected at any time. Notice is provided to staff at logon to CFPB systems through a warning page.

For information not collected directly from individuals, such as information collected during investigations, CFPB provides constructive notice of the CFPB's information practices through the CFPB privacy policy, this PIA, and the associated SORNs.

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

Where required, the Bureau will provide notice to individuals about how their information is shared.

In some cases, such as information collected pursuant to discovery or a related court order, individuals may not receive notice as to how information will be used or disclosed. In these cases, the use and disclosure of information is controlled by applicable federal law, discovery rules, and court orders.

In cases where notice cannot be provided or is not required, the CFPB has provided constructive notice of how it will share information stored in the LIST in SORNs, through this PIA, and through the Bureau's privacy policy. Section 2.1 has more information about how notice of the collection and use of information in the LIST is provided to individuals.

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?

Some individuals may not be directly notified that their information is collected and maintained in the LIST, as such notice would compromise pending investigations and the underlying investigative purpose of the LIST.

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 LIST may collect, maintain, and process any information that the CFPB obtains as part of its law enforcement and litigation activities. The complete list of categories of individuals covered by this system is available in the related SORNs for the systems. In general, the LIST includes information about:

- Subjects of CFPB's enforcement activities;
- Individuals and entities with information that may be relevant to CFPB investigations;
- Individuals who are or were customers or individuals who had been solicited by covered institutions; Other individuals involved in litigation regarding civil and criminal matters within the jurisdiction of the CFPB either as plaintiffs or as defendants or involved in administrative complaints filed against or by the CFPB;
- CFPB employees and contractors who use the LIST.

3.2 What PII will the system include?

The LIST may include PII about the individuals outlined in Section 3.1. A complete list of what information, including PII is collected and stored by the LIST is available in the related SORNs. In general, information includes:

- Financial transaction data (including consumer transaction data);
- Narratives and other information in complaints filed through the CFPB Consumer Response database[4];
- Banking records;
- Credit reports;
- Contracts;
- Employee records;
- Names;
- Titles;
- Account and credit card numbers;
- Social Security numbers;
- Tax identification numbers;
- Addresses;
- Phone numbers;
- Email addresses; and
- Date of birth.

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

Various laws and regulations require or permit the Bureau to conduct investigations, take enforcement actions, represent itself in litigation, and carry out special projects. The LIST allows Bureau employees to collect, maintain, and analyze information in support of these purposes.

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 LIST will be used to aggregate data from multiple sources in support of investigatory and enforcement actions. This aggregation may result in the creation of new evidentiary information about an individual, which may be used in enforcement actions.

[4] The Consumer Response System PIA is available at http://files.consumerfinance.gov/f/2012/01/CFPB_PIA_Consumer-Response.pdf.

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

The LIST protects information, whether aggregated or not, as described in Section 6, Security, below.

3.6 Will the system monitor the public?

The LIST does not monitor the public directly although components of the LIST can be used to gather information on certain activities of subjects of interest within the jurisdiction of the Bureau.

3.7 Will the system monitor employees or contractors?

The system monitors employee use to track usage and identify potential misuse. Specifically, the investigation lab requires employee usage, including dates and times of usage and reason for use.

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

Components of the LIST can produce reports to support the various purposes of the LIST. These reports may be for administrative, analytic, investigative, or enforcement purposes and will often include PII on individuals.

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

The LIST collects, processes, and stores large volumes of information, including PII and other sensitive information, which is obtained from various sources. There are two risks directly involved with the volume of PII collected and stored within the LIST, the first of which is addressed below. The second risk, which is related, is covered in Section 6.

There is a risk that documents or other information provided by companies to the CFPB or collected during discovery or through forensic analysis, civil investigative demands ("CIDs"), investigations, or other means could contain unnecessary PII about individuals.

Because some of the essential information required for the Bureau's enforcement of consumer financial statutes and regulations will contain PII this overall risk is acceptable. The Bureau has appropriate technical controls and policies and procedures in place, which restrict access to PII collected through an investigation or as part of litigation.

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?

As discussed above in Sections 1.1 and 3.3, information in the system is used to support the CFPB's law enforcement and general litigation activities, including to investigate and enforce federal consumer financial statutes and regulations and to defend against suits brought against the Bureau. As outlined in Section 3.9, some documents provided to or collected by the CFPB as a result of a CID, discovery, forensics, through investigations, or voluntarily provided could include unnecessary PII or PII not intentionally requested or collected by the Bureau.

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 LIST with external parties to fulfill its enforcement responsibilities, to defend itself in litigation, or pursuant to statutory or regulatory requirements. In some cases, the Dodd-Frank Act requires us to share this information. In other cases, we have chosen to share information with other government agencies. The specific methods of how the information will be shared will be different depending on the particular type of information and the purpose for which it was collected. The related SORNs will define in more specific detail how this information will be shared.

Parts of the LIST may be accessed by authorized contractors, law enforcement partners, and other state and federal agencies the Bureau has partnered with to enforce consumer financial laws. The CFPB may also share information with courts, opposing counsel, defendants, expert witnesses, or other individuals as otherwise authorized by the law, although these entities and individuals do not have access to the LIST themselves.

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

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

When the CFPB collects PII about individuals who are involved in CFPB investigations, civil or administrative actions, or in litigation involving the Bureau, it may collect such information directly from those individuals or it may collect such information from a company who is the subject of research, investigation or an enforcement action, or a party in the litigation. Additionally, it may collect information from third parties including existing federal databases, other agencies responsible for related regulatory functions, or from publicly available sources such as Internet searches or publicly available data sources.

Information may be provided to the CFPB for the LIST voluntarily, via compulsory process, discovery, through on-site collection, through other investigative sources, or from internal sources.

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

The LIST is a collection of systems and processes, some of which are standalone others are connected.

Some components of the LIST are comprised of systems maintained by through the Department of Justice (DOJ) to effectively store, process, transmit and maintain critical information on behalf of participating federal agencies. These systems are tightly controlled by contractual stipulations, CFPB security standards, and FISMA requirements; once these requirements are met, access may be granted to any CFPB employee with a bona fide need to know. If access has been granted, information is retrieved via random, user-generated queries. Information is via industry-standard HTTPS encryption protocols.

Within the CFPB, components of the LIST will connect directly to the Bureau's shared network drive for document management, and with the Matters Management System to provide support to the matters tracked under that system.

Other components of the LIST will be stand-alone and not connected to other systems for forensic purposes or for purposes of preserving the anonymity of investigations.

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?

Information that is used by the CFPB as part of its law enforcement and litigation activities is reviewed for accuracy and timeliness as required by the particular activity. In some cases, CFPB staff may research the information that is obtained to ensure that it is timely and accurate. In some cases, the individual submitting the information may also be required to certify the accuracy of the information (e.g., witness or financial statements in court cases). Because in most cases individuals do not submit their own personal information to the LIST it is not always possible to ensure completeness. However, to the extent that it is relevant the Bureau makes every effort to ensure that information is appropriately complete.

In other cases, such as the collection of information from the Internet through the Bureau's investigations, information will not be systematically checked for accuracy and timeliness. Information available on the Internet is subject to continuous change. Therefore, information

that is collected by users from the Internet is considered an accurate representation of the content as of the point-in-time it was collected and may be required to be maintained as such for research and investigative purposes. That is, the Bureau may collection information from the Internet during investigation where the information is factually incorrect but it is an accurate representation of the information on web site investigated at that point-in-time.

Information in the LIST is subject to appropriate security and chain-of custody controls (policies, procedures, and technical and physical controls) as appropriate. These controls ensure that sensitive information is protected from any undue risk of loss, and that the contents of evidentiary materials remain unchanged from the point-in-time they are included in the LIST. These controls provide the CFPB the ability to verify that information stored within the LIST has not been changed.

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?

There are no risks associated with the data quality or integrity of the information collected or used by the LIST.

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?

Internally, the Bureau restricts access to the LIST primarily to law enforcement personnel (e.g. attorneys, forensic accountants, investigators, paralegals) and technologists. The LIST will also be used by staff in other offices (e.g. the Legal Division, the Front Office, the Freedom of Information Office.)

In some limited cases, access is granted to external parties for the purpose of multi-tenant review or collaboration on investigations or enforcement actions.

LIST users must demonstrate a *bona fide* need for access to carry out their assigned job responsibilities. The CFPB limits the extent of access depending upon whether individuals need to see certain information or use certain tools to perform their job responsibilities.

Access is managed by the issuance of non-transferrable access codes and passwords to authorized staff who have completed any relevant training specific to the component they are seeking access to, or signed any relevant user agreements, rules of behavior (or similar documents) for the component. Some of the information in the LIST 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.

Much like initial access, revoking access can occur for each individual component of the LIST, and occurs when an individual no longer demonstrates a need for access, upon termination of that employee, or upon employees changing job duties within the Bureau.

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

The CFPB, or the organization responsible for the LIST component, has evaluated each component and either completed a system security plan or revised an existing system security plan to incorporate the component. Any new component added to the LIST will be evaluated before use and a system security plan developed or revised, as appropriate.

6.3 How will the system be secured?

Information in the LIST is protected through robust security controls within the environment, and the use of secure network protocols for transmission of data outside the environment. Required security for each component is derived from the sensitivity of the information within that component. For example, some components of the LIST require multiple authentications for access by requiring users to provide a unique user ID and password in two places. Certain components of the LIST can prohibit users from downloading or sharing information.

The LIST components are regularly monitored and audited to identify any unauthorized access attempts, to verify the appropriate access level have been granted to users, and to identify any potential misuse of the component, or violation of applicable policies, procedures, or rules of behavior.

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

Currently, the CFPB relies on the Treasury's Network for monitoring malicious activity and alerting when this activity is found. For the components of LIST that are not connected to Treasury, activity is recorded and these files are sent to CFPB's Computer Security Incident Response Team for review. 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.

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 a central, collaborative web repository will attract hackers, identity thieves, and other cyber-threats.

As discussed above, the LIST provides users with computing resources and tools in an environment that is tailored to the processing needs and security risks inherent in the information to be accessed and processed, or to the component which is being utilized.

Once processed in the LIST, information that is appropriate to be placed on the General Support System ("GSS") is copied to the CFPB's production network and made available for search and review by case teams in the production network. Other data may remain available for search and review by case teams within the LIST. Information in the production network portion of the LIST is protected by the technical and procedural controls of the CFPB's GSS. Access is restricted to authorized users, including security monitoring, auditing, and remote access controls in CFPB's GSS.

For cases where the CFPB has authorized a third party to use the LIST in order to process information in the system, controls include the use of appropriate confidentiality and non-disclosure agreements, coupled with a review of the vendor's operation, and the receipt of sufficient assurances as to the procedures that will be used to assure the security and confidentiality of the information.

Information obtained in physical format or electronically stored on removable media is subject to CFPB polices for handling and safeguarding PII. In addition, the CFPB has adopted and published detailed procedures for managing information that it receives in physical form.

These controls serve to mitigate the privacy risks associated with information once it is received by the CFPB. To address the risks associated with transportation of electronic data to and from the CFPB, the agency requires that data be encrypted with National Institute of Standards and Technology ("NIST") certified cryptographic modules, when possible. When encryption is not feasible due to technical limitations or cost, or the information is provided in physical format, the agency requires the use of alternative controls that are tailored to the risks associated with the data being transferred.

The CFPB has implemented procedures that require management authorization prior to shipping sensitive information outside the agency, as well as the maintenance of records of the information being shipped and its destination.

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.

Individuals that provide the CFPB with information on a voluntary basis may choose to decline to provide such information (e.g. consumer complaints, voluntary disclosures, whistleblowers). However, individuals do not have a right to decline to provide information that is required by law such as via compulsory process, or in cases where information is gathered from public sources as part of the investigatory process. Moreover, individuals generally do not have a right to consent to particular uses, including dissemination of the information stored in the system.

Moreover, a large portion of the data collected by the system is provided by organizations pursuant to applicable laws and regulations rather than directly from individuals or through investigatory means which may include the collection of publicly available information.

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 at www.consumerfinance.gov/foia. It is important to note that because some information in the LIST is of a law enforcement nature, it may not be able to be accessed or changed if doing so would negatively impact or otherwise harm a pending investigation or enforcement action, or compiled in reasonable anticipation of a civil action or proceeding.

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

More information about access and amendment 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 LIST, or to update or correct information submitted.

This risk is acceptable because the enforcement of consumer financial statutes and regulations by the Bureau is mandated by the Dodd-Frank Act and because allowing individuals access to or amendment of certain records may impede the Bureau's ability to meet this mandate. Moreover, much of the information collected in the LIST is collected pursuant to applicable laws and regulations such as via compulsory process.

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 provides privacy and security training to all employees of the CFPB, including contractors who handle PII on behalf of the CFPB. Additionally, each of the components in the LIST will have additional user training for proper use of the tool.

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 worked to implement a rigorous set of security controls, including policies and procedures around the LIST, and has limited access to those with a *bona fide* need-to-know.

The use of LIST components will be audited either directly by a LIST component, or when that is not possible, through other technical auditing mechanisms. Audit logs will be reviewed on a regular basis based on how LIST components are used.

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?

There are no risks associated with accountability and auditing of this system.