Privacy Impact Assessment Template

CYBER INVESTIGATIONS UNIT (CIU) LAB
(SYSTEM NAME)

AUGUST 31, 2020
DATE

FHFA-OIG's Chief Counsel handles certain tasks commonly undertaken by an agency's Senior Agency Official for Privacy (SAOP). This template is used when FHFA-OIG's Chief Counsel determines that an FHFA-OIG IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the FHFA-OIG Chief Counsel for review and coordination with the agency SAOP.

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how Personally Identifiable Information (PII) is collected, stored, maintained, and shared. A PIA must be completed when FHFA-OIG: 1) develops or procures an IT System or project that collects, maintains, or disseminates PII from or about members of the public; or 2) initiates a new electronic collection of PII for 10 or more members of the public. System Owners are primarily responsible for completing the PIA with assistance from FHFA-OIG's IT developers, IT security officers, and Office of Counsel.

Below is guidance, by section, for a System Owner to follow when completing a PIA.

OVERVIEW SECTION

- Provide a thorough, complete, and clear overview of the System and give the reader the appropriate context to understand the responses. Some questions to consider include:
  - What is the purpose of the System?
  - What will be the primary uses of the System?
  - How will this support the Division's/Office's/Program's mission?
- This section fulfills the E-Government Act's requirement for an introduction to members of the public who may be reading the PIA. PIAs may be made publicly available unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information.

FOR A FULL PIA

- **COMPLETE ALL SECTIONS**

FOR A MODIFIED PIA - Under certain circumstances the FHFA-OIG Chief Counsel may make a determination that a complete PIA is not necessary depending upon the nature and extent of the PII collected. When the Chief Counsel makes such a determination, the System Owner only needs to complete the following sections of the PIA template:

- **OVERVIEW**
- **SECTIONS 1, 2, AND 6**

SECTION 1.0 CHARACTERIZATION OF THE INFORMATION

- Identify if the System contains information about individuals, versus statistical, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.
- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question to consider:
  - Where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, or a private organization).
- If the System collects information from 10 or more members of the public, ensure that FHFA-OIG has received prior approval from OMB to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the FHFA-OIG Office of Counsel for assistance.

SECTION 2.0 USES OF THE INFORMATION

- Identify the primary uses of the information and how the information supports FHFA-OIG's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted to a limited number of staff who use the data for their specific program use.

SECTION 3.0 RETENTION

- The Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).
- The retention periods for data/records that FHFA-OIG manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule, to which FHFA-OIG is subject. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA-OIG's Office of Administration (OAd).
- Disposing of the data at the end of the retention period is the last state of life-cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

SECTION 4.0 NOTICE, ACCESS, REDRESS AND CORRECTION

- The Privacy Act requires that "each agency that maintains a System of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. 552a(e)(1).
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the System retrieves information by an individual's name or other unique identifier (e.g. social security number) it is a Privacy Act System and will need a SORN published in the Federal Register. The System may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact FHFA-OIG's Office of Counsel.
- If a name or other unique identifier is not used to retrieve information, it is possible that the System is not a Privacy Act System. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may still be protected from disclosure under the Freedom of Information Act.
- FHFA-OIG is subject to FHFA's agency specific Privacy Act Rule published in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors, if appropriate.
- Any employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000.

SECTION 5.0 SHARING AND DISCLOSURE

- If you do not know whether or not Systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist between the Systems/applications. As an example, if your System/application shares data with another System/application, ask yourself

whether you have access to the data in the interfaced System/application. If so, then your answer is yes and an explanation is needed.

- Also consider "other" users who may not be obvious as those listed, such as GAO. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN under the "Routine Use" section when a Privacy Act SORN is required. The more comprehensive the list, the better it is.
- You must first review the SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are restrictions on the use and disclosure of information that are set forth in a SORN.

SECTION 6.0 ACCESS AND SECURITY

- Access to data by a user (i.e. employee or contractor personnel) within FHFA-OIG is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.
- The criteria, procedures, controls and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.
- The System owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open Systems" where all information can be viewed by all users. System administrators may be afforded greater access – i.e. to all of the data – depending upon the System and/or application. However, restrict access when users do not need to have access to all the data.
- When a contract provides for the operation of a System on behalf of FHFA-OIG, the Privacy Act requirements must be applied to such a System. Contact the Contracting Officer or Contracting Officer's Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The Security Assessment and Authorization (SA&A) process requires a System security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of Systems to ensure that only authorized users can access the System for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the System can in fact monitor use of the System. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are System-based means by which the ability to access a System is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of System activity and user activity including invalid logon attempts, access to data and monitoring. The SA&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.
- Every System/application/process that uses data must have controls in place to prevent the misuse of the data by those having access to the data.
- All employees, including contractors, have requirements for protecting information in Privacy Act Systems. Describe the controls in place, including any privacy and security awareness controls such as training materials, to protect the information.

PIA FORM

Overview

This section provides an overview of the System and addresses the following:

- The System name and the division/office that owns the System;
- The purpose of the program, System, or technology and how it relates to the agency's mission; and
- A general description of the information in the System.

Date submitted for review: August 28, 2020

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office Phone Number**
Paul Conlon	Paul.Conlon@fhfaoig.gov	Office of Investigations	202-730-4752
Kyle Lin	Kyle.Lin@fhfaoig.gov	Office of Investigations	202-730-4914

System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to FHFA-OIG's mission.

The CIU Lab supports the FHFA-OIG Office of Investigations. CIU forensic examiners and agents use the CIU Lab to collect and analyze data, to conduct digital forensics for FHFA-OIG, and to provide support for outside law enforcement investigations. The CIU Lab is comprised of multiple standalone, off-network systems that CIU forensic examiners and agents use to analyze evidence and data, and create digital forensic reports for law enforcement activities.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, System, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is being collected, used, disseminated, or maintained in the System?	The information maintained in the system is digital investigative evidence such as financial records, loan information, contact information, and other information required to conduct investigations and further the OIG's mission in areas of: • Criminal law enforcement activities; • Administrative investigative matters; • Conducting analysis concerning subjects of investigative or other interest; • Conducting analysis to identify previously unknown areas of note, concern, or pattern; • Litigation support; • Data analysis; • Evaluation and testing of software; • Assembly of information that summarizes and describes evidence; and • Assembly of information that describes testing of the evidence, including forensic procedures, standards, controls, instruments, observations, test results, and documents created by the forensic examiner (e.g., charts, graphs, photos), which support the examiner's conclusions. All information collected is maintained outside the FHFA-OIG network in standalone systems. The data is inaccessible unless a person is physically in the CIU Lab.
1.2	What or who are the sources of the information in the System?	Information in the CIU Lab is collected from other FHFA-OIG systems and other external sources. Some information in those systems may have been collected from individuals, such as crime victims, witnesses, and members of the public. Other information may be provided by other law enforcement agencies, private sector entities, and open source intelligence (such as the internet and other electronic forms of information.) Information on FHFA and FHFA-OIG employees

#	Question	Response
		is generally collected directly from the employee unless the employee is the subject of an investigation. In that case, the employee is treated as any other individual under investigation, and it is often necessary to acquire information from sources other than the individual. (At times, vital information can only be obtained using legal processes from other sources that are familiar with the individual and his/her activities.)
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	• For criminal law enforcement activities; • For administrative investigative matters; • To conduct analysis concerning subjects of investigative interest; • To conduct analysis to identify previously unknown areas of note, concern, or pattern; • For litigation support; and • For testing and evaluation of software.
1.4	How is the information provided to FHFA?	Data is provided to the FHFA-OIG Office of Investigations from external sources, and from systems maintained by the FHFA-OIG OIGNet GSS. Data is transferred from other systems to encrypted devices, and then uploaded to the CIU system for use only by personnel with permission to receive and view the data. None of these external sources or OIG systems are able to electronically share data with the CIU lab; information must be manually uploaded because the CIU lab is a standalone system.
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss, or compromise of the information will/can affect an individual's privacy.	Risks to an individual's privacy are that personal, financial, and other information may be subject to disclosure and compromise, as well as the fact that an individual is or may be the subject of or associated with a criminal or civil investigation by FHFA-OIG or other law enforcement entity.
1.6	If Social Security numbers are being collected, provide the legal authority for the collection. In addition, describe in detail the business justification for collecting SSNs, what the consequences would be if SSNs were not collected, and how the SSNs will be protected while in use, in transit and in storage.	The Inspector General Act of 1978 and the Inspector General Empowerment Act of 2016 authorize the collection of Social Security Numbers (SSNs) for law enforcement investigations. SSNs are often necessary in the law enforcement context to reliably identify investigation subjects and witnesses. The consequences of not collecting SSNs are the potential misidentification of an individual or

#	Question	Response
		witness in the course of an investigation, which could undermine the reliability and integrity of the investigation results, and result in inefficiency and potential errors concerning vital criminal evidence. SSN data will be protected in accordance with NIST 800.53, FIPS 199, other relevant NIST information security standards, and Special Publications.

Section 2.0 Uses of the Information

The following questions delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	How will the information be used and for what purpose?	The information will be used for the following mission-critical functions of FHFA-OIG: • For criminal law enforcement activities; • For administrative investigative matters; • To conduct analyses concerning subjects of investigative interest; • To conduct analyses to identify previously unknown areas of note, concern, or pattern; and • For litigation.
2.2	Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	The information is secured in accordance with FISMA requirements. At the time of this PIA, the most recent Authority to Operate for the CIU Lab was issued on 04/20/2020. Auditing procedures are in place to ensure compliance with security standards. The CIU lab is in a secured area that requires permission to access through electronic means (i.e. having the security code to open the access door, which is granted to only a few OI personnel.) Enforcement of established physical security capabilities (management walk-throughs and assessment of security locks, doors, storage materials, and access control systems that monitor individuals requesting facility access). Physical access is strictly controlled both at the perimeter and at the lab ingress point by video surveillance, intrusion detection systems, and other electronic means. The risk of inappropriate use of information is further mitigated with auditing to monitor user activities. The use of these controls in combination with policy and procedural controls, including privacy and security training, acknowledgement of Rules of Behavior, use of level of review of information, and, if necessary, disciplinary action, protects the privacy of information in the CIU Lab.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	See 3.2
3.2	Has a retention schedule been approved by FHFA's Records Management Office and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	All FHFA-OIG records are subject to FHFA's Comprehensive Records Schedule. The CIU Lab may contain a variety of records, subject to varied retention periods. Potential disposition of records maintained in the CIU Lab will be evaluated on a case-by-case basis to determine the appropriate retention period for each record.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There is low risk associated with the length of time the data is retained in the CIU lab. While not in use, the data is encrypted, and only CIU members have physical access to the lab. The data retention time is dependent on FHFA's Comprehensive Records Schedule as well as on the length of time for litigation related to criminal and civil investigations. Permission (such as Grand Jury Lists pursuant to the Federal Rules of Criminal Procedure, assignment to the CIU) will be required to access the data and will not be granted without appropriate need-to-know and training.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	No. A SORN is not required for the CIU Lab. The CUI lab is not a group of records under the control of FHFA-OIG from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The CIU Lab obtains information through the physical transfer of data on encrypted drives and does not have an automated system for pulling various records by an individual's name or unique identifier. To the extent that data entered in the lab's systems originates from other systems of record, those systems of records have their own applicable SORNs (e.g., FHFA–OIG Investigative Files

#	Question	Response
		Database and FHFA–OIG Investigative MIS Database). Personal information and records provided to the CIU Lab are not stored, maintained, or retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the CIU Lab is not a database or database management system, and although various components may contain PII, the OIG Lab does not function as a group of records from which information is or can be retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	The CIU Lab does not solicit information from individuals; therefore, the notice requirements in 5 U.S.C. 552a (e)(3) are not applicable.
4.3	Do individuals have the opportunity and/or right to decline to provide information? What are the consequences if an individual declines to provide the information?	The CIU Lab does not solicit information from individuals.
4.4	What are the procedures that allow individuals to gain access to their information?	FHFA-OIG has issued regulations and established processes under the Freedom of Information Act (FOIA) and Privacy Act for individuals to request Agency records.
4.5	What are the procedures for correcting inaccurate or erroneous information?	Information is inputted and maintained by CIU Examiners and Agents, who are responsible for ensuring the information is up-to-date and accurate. Any discrepancies or errors identified will be corrected by the CIU Examiner/ Agent. Further, the proper maintenance of files and data accuracy are elements of the performance review process for the CIU Examiners. Because the CIU Lab is not a system of records, there is no process for individuals to seek access to CIU Lab records or correct inaccurate records. However, to the extent data entering the lab originates from FHFA-OIG systems of records, these systems have processes for individuals to

#	Question	Response
		access and correct records (e.g., FHFA–OIG Investigative Files Database and FHFA–OIG Investigative MIS Database). For an individual who requests a correction of FHFA-OIG records, OIG will follow procedures in FHFA's Privacy Act regulation (see 12 C.F.R. 1204.3(d)).

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	CIU Lab information may be shared with other FHFA-OIG offices as needed, to further effort of audit, evaluation, and compliance activities. Audit, evaluation, and other OIG personnel will ensure that efforts are not duplicated, and that law enforcement activity is not compromised by inadvertent disclosure during the conduct of an audit or evaluation.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	CIU Lab information may be shared with other law enforcement agencies, including U.S. Attorney's offices, state prosecutors, and state and federal law enforcement agencies (including other OIGs) with whom a joint investigation is being conducted. Other releases may be to members of the general public or media, in response to FOIA requests. All releases under FOIA will include the redactions for exemptions under 5 U.S.C. § 552(b).
5.3	Is the sharing of PII outside FHFA-OIG compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA-OIG.	Yes. Currently, OIG shares PII in accordance with the routine uses set forth in FHFA-OIG's published SORNs. https://www.gpo.gov/fdsys/pkg/FR-2013-11-01/pdf/2013-26010.pdf.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	Risks (as described in Section 1.5) may include the compromise of data when shared with an external source, either inadvertently through a breach or other compromise, or a deliberate release of information. Open case information from the CIU Lab is shared with other law enforcement entities with existing PII controls and protection infrastructures, (i.e.,

#	Question	Response
		the Department of Justice.) All information transferred is password encrypted and is provided with the notification that the material may not be disclosed without the prior authorization of OIG. Closed case file information is also password encrypted and only disclosed to authorized recipients on-site at OIG; the material cannot be removed or copied without OIG permission. The viewing party must submit a written acknowledgement of OIG's control over any disclosure of the information, and this acknowledgement is made part of the case file.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing? **If so, provide a signed copy to the Chief Counsel with this PIA.**	Access to the CIU Lab is restricted to authorized users. Those authorized users are identified by the Deputy Inspector General for Investigations and are limited to those assigned to the CIU and the CIU managers. Procedures are documented in the official OI manual.
6.2	Will non-FHFA-OIG personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will FHFA-OIG control their access and use of information? Are there procedures documented in writing? **If so, provide a copy to the Chief Counsel with this PIA.**	At this time, non-OIG personnel do not have access to the CIU Lab. Future needs will determine any changes to the access policy, and all changes will be approved by the Deputy Inspector General for Investigations. Procedures are documented in the official OI manual.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System?	Basic user training is conducted upon assignment to the Office of Investigations. This training includes assignments of passwords and log-on information. CIU Lab personnel receive additional training on how to safely and securely access information in the CIU Lab. Ongoing training is conducted on a regular basis, but at least annually.
6.4	Describe the technical/administrative safeguards in place to protect the data?	See Section 2.2 for detailed technical information on controls and safeguards.

#	Question	Response
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Local device audit logs, physical access logs, and surveillance video will be periodically reviewed by the CIU Lab Manager.
6.6	Has a SA&A been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provided the expected completion date of the SA&A.	A SA&A was completed on 04/15/2020.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? **Provide a copy to the Chief Counsel with this PIA.** If not, when do you anticipate such ATO being issued?	An ATO (Ongoing Authorization) was issued on 04/21/2020 and will remain in effect until the completion of the next annual assessment and subsequent authorization decision (completed within 90 days from the issuance of the next annual Security Assessment Report).

Signatures

FHFA-OIG:

Paul Conlon System Owner (Printed Name)	PAUL CONLON Digitally signed by PAUL CONLON Date: 2020.08.31 09:51:15 -04'00' System Owner (Signature)	Date
Executive Sponsor (Printed Name)	Executive Sponsor (Signature)	Date
System Developer (Printed Name)	System Developer (Signature)	Date
Michael Stoner Chief Information Security Officer (Printed Name)	MICHAEL STONER Digitally signed by MICHAEL STONER Date: 2020.08.31 09:46:17 -04'00' Chief Information Security Officer (Signature)	Date
Michael Smith Chief Information Officer (Printed Name)	MICHAEL SMITH Digitally signed by MICHAEL SMITH Date: 2020.08.31 10:02:08 -04'00' Chief Information Officer (Signature)	Date
Leonard J. DePasquale Chief Counsel (Printed Name)	LEONARD DEPASQUALE Digitally signed by LEONARD DEPASQUALE Date: 2020.08.31 10:09:16 -04'00' Chief Counsel (Signature)	Date

FHFA:

David A. Lee	DAVID LEE Digitally signed by DAVID LEE Date: 2020.09.01 10:35:53 -04'00'	
Senior Agency Official for Privacy (Printed Name)	Senior Agency Official for Privacy (Signature)	Date