



Privacy Impact Assessment Template

MICROPACT I-COMPLAINTS

11/6/2014

This template is used when the Chief Privacy Officer determines that an IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the Chief Privacy Officer.

David A. Lee
Chief Privacy Officer
Senior Agency Official for Privacy
Federal Housing Finance Agency
400 7th Street SW
Washington, DC 20024
(202) 649-3803
Privacy@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form (“IIF”; also referred to as Personally Identifiable Information (PII)) is handled. PIAs are to be completed when FHFA: 1) develops or procures an IT System or project that collects, maintains, or disseminates IIF from or about members of the public; or 2) initiates a new electronic collection of IIF for 10 or more members of the public. PIAs are not required for collections of information from Federal employees. IIF about government personnel generally is protected by the Privacy Act; however the Office of Management and Budget (OMB) encourages agencies to conduct PIAs on these Systems, as appropriate. System Owners and Developers are responsible for completing the PIA.

The guidance below has been provided to help System Owners and Developers complete a PIA.

Overview

- In this section, provide a thorough 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 for 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 PIA COMPLETE ALL SECTIONS.

FOR A MODIFIED PIA COMPLETE THE FOLLOWING SECTIONS ONLY:

- 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 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 Office of General Counsel for assistance.

Section 2.0 Uses of the Information

- Identify the primary uses of the information and how the information supports FHFA's or the Office's/Division's/Program'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 manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA's Records Management Office.
- 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 may 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 the Chief Privacy Officer.
- 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.
- The agency has developed and published an agency specific Privacy Act Rule 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 the General Counsel Accountability Office or the FHFA Office of Inspector General. "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 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 access 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, 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.
- According to OMB Circulars A-123 and A-130, 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. For instance, in computerized Systems the Security Information Record (SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the System and is transparent to the user. Describe these processes in response to this question.
- 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: 10/23/2014

System Name: MicroPact iComplaints			
System Owner(s)			
Name	E-mail	Division/Office	Office Phone Number
Brian Guy	Brian.guy@fhfa.gov	OMWI/EEO Services	202-649-3019
System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to the agency's mission.			
<p>The software will organize, track, and update data required for the EEOC's Form 462 Report as well as the No Fear Act Report. It also tracks all aspects of the EEO complaint process through unique case identifiers and a schedule of important processing events related to a case. In essence, the captured data consists of employee names, former employees, applicants, contractors involved in the EEO process, the alleged responsible management officials, and witnesses. The database contains information regarding the issues in each case and related factors such as race, national origin, disability, etc. The database will house investigative reports, settlement agreements, and case decisions. These documents may contain social security numbers, personal addresses, phone numbers, and work records of employees, former employees, applicants, and contractors. The agency is charged with preventing and addressing discrimination. This software allows the agency to file reports, manage cases, and identify trends which can be subsequently addressed.</p>			

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 collected, used, disseminated, or maintained in the System?	Equal Employment Opportunity (EEO) complaints, settlements, medical records, personnel records, disciplinary records, names, addresses, phone numbers, date of birth information, age and ethnicity and Alternative

#	Question	Response
		Dispute Resolution matters.
1.2	What are the sources of the information in the System?	Agency officials, OHRM records, employee testimony, medical professionals, current and former employees, investigative reports documentation and affidavits.
1.3	Why is the information being collected, used, disseminated, or maintained?	Equal Employment Opportunity Commission (EEOC) complaint and hearing process.
1.4	How is the information collected?	Through interviews, investigations, and document requests.
1.5	Given the amount and type of data collected, what risks to an individual's privacy are associated with the data?	Moderate. The system will be used by a few users who will safeguard the information and there are security features in place, such as data encryption, password protection, role-based access controls, etc.

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	Describe the uses of information.	Reporting to the EEOC and Congress, resolving complaints, completing hearing records, and training purposes.
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.	Information is redacted for training and reporting purposes. The software has security features in place. Only a few users have access to the system.

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 information retained?	Depends on the case. Once the case is resolved the record should be destroyed four years after case resolution.

#	Question	Response
3.2	Has a retention schedule been approved by FHFA's Records Management Officer and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes, 5.3b Human Resources Records.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	If files are accessed by inappropriate personnel or if EEO case information is lost, sensitive data about agency management decisions, disciplinary actions and employee EEO activity may become available to those outside the EEO process. Such a breach would compromise trust in the EEO process and the confidentiality of that process. The agency redacts PII and sensitive data in complaint files. When possible case numbers are used in lieu of complaint names. Data is stored in a secured closet and files are securely maintained electronically. Access to the I-complaints system is limited to those with a password. Only a few employees have access to EEO materials.

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.	Yes. EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records
4.2	Was notice provided to the individual prior to collection of information?	Yes
4.3	Do individuals have the opportunity and/or right to decline to provide information?	Not if the individual wants the case processed in the Formal EEO complaint process.
4.4	What are the procedures that allow individuals to gain access to their information?	They get a copy of the Counselor's report and the Report of Investigation (ROI). Also, they may file a request under the Privacy Act using the procedures set forth in FHFA's Privacy Act

#	Question	Response
		regulation – 12 CFR 1204.
4.5	What are the procedures for correcting inaccurate or erroneous information?	The reports are reviewed by the employee and they can request changes with the agency. At the hearing stage the employee can request changes to the record with the Administrative Judge. Changes may also be made under the procedures set forth in FHFA’s Privacy Act regulation – 12 CFR 1204.

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?	If a hearing is requested OGC is provided with the ROI and complaint file, as they defend the agency in EEO matters and OHRM is provided with the name of the employee for data requests. Settlement agreements are shared with OHRM and OBFM for processing. The agency Director is aware of settlement agreements and high profile cases. Management officials and witness become aware of pending investigations in which their testimony is required.
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.	EEOC is provided with complaint files, reports which include agency demographics, case type, complaint issues, settlement/ADR and case processing times are provided. Congress also receives reports with similar information. Federal courts may also receive the complaint file. OIG gains access to EEO information during audits and investigations.
5.3	Is the sharing of PII outside the agency 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.	Yes. This information may be disclosed to the appropriate federal state or local agency. It may be disclosed to Congressional offices. The contract investigator and/or counselor is authorized by the agency to carry out its responsibilities under 29 CFR 1614. Former employees and applicant witnesses may become aware of information under this CFR as well
5.4	Given the external sharing, explain the privacy risks identified and describe how they were/are mitigated.	Sensitive details of EEO complaints may become available to parties without a need to know. This may include contact information, medical documentation, and disciplinary actions. Pertinent information is redacted. Complaint

#	Question	Response
		files are sent securely to the EEOC via electronic means. Investigation information is sent via the agency's secured system. The reports shared externally do not request PII from individual complainants. The reports only identify general case information such as case processing timeframes, the issue(s), and basis.

Section 6.0 Technical Access and Security

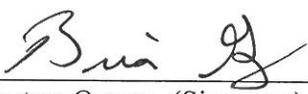
The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing? <u>If so, attach a copy to this PIA.</u>	The MicroPact iComplaints Access Control and Audit Procedures define procedures for requesting and granting access to the system, and for assigning roles based on the concept of least privilege. A copy of the procedures is attached.
6.2	Will non-FHFA 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 the agency control their access and use of information? Are there procedures documented in writing? <u>If so, attach a copy to this PIA.</u>	Only FHFA employees and possibly contractors specifically authorized by the iComplaints system owner will have access to the data. Access will be granted in accordance with the MicroPact iComplaints Access Control and Audit Procedures. Additionally, vendor representatives may have access to the system in order to perform maintenance and troubleshoot technical issues. A copy of the procedures is attached.
6.3	Describe the training that is provided to users either generally or specifically that is relevant to the program or System?	The vendor will provide the training both functional and technical end user or train the trainer. This is an agreed upon training.
6.4	What technical safeguards are in place to protect the data?	The MicroPact iComplaints system completed the Federal Risk and Authorization Management Program (FedRAMP) and received a FedRAMP authorization on June 6, 2014. The system was assessed at the FIPS-199 Moderate Impact level. FedRAMP requires that all cloud vendors implement a set of controls beyond the requirements of NIST SP 800-53 Revision 4. Further, FHFA has developed the MicroPact iComplaint Access Control and Audit Procedures to define how FHFA privileged users securely manage user accounts and monitor user behavior.

#	Question	Response
6.5	What auditing measures are in place to protect the data?	As described in the MicroPact iComplaints Access Control and Audit Procedures, the iComplaints system captures logs of all user actions on the system, and at least monthly, the system owner will review events from the last 30 days and notify IT Security when the logs have been reviewed, noting if any unusual activity was observed.
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.	iComplaints received FedRAMP Authorization on June 6, 2014. The FHFA Agency Authorization is scheduled to be completed by November 7, 2014.

Signatures

Brian Guy
System Owner (Printed Name)


System Owner (Signature)

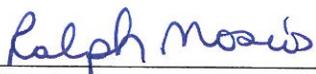
11/6/2014
Date

N/A
System Developer (Printed Name)

System Developer (Signature)

Date

Ralph Mosios
Chief Information Security Officer
(Printed Name)


Chief Information Security Officer
(Signature)

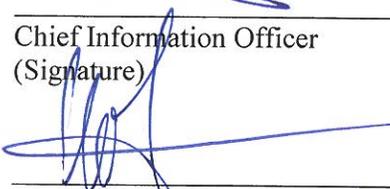
11/6/2014
Date

R. Kevin Winkler
Chief Information Officer
(Printed Name)


Chief Information Officer
(Signature)

11/6/2014
Date

David A. Lee
Chief Privacy Officer
(Printed Name)


Chief Privacy Officer
(Signature)

11/7/2014
Date



Federal Housing Finance Agency
Access Control and Audit Procedures

For

MicroPact iComplaints

Release Date: Sep 25, 2014

Approved

Brian G. J.

11/6/2014

Prepared By:
FHFA IT Security

Non-Public Information

NON PUBLIC INFORMATION

Table of Contents

- 1. Scope of this Document 2
- 2. Introduction 2
- 2.1. iComplaints FHFA Administrators 2
- 3. Access Control Process 3
- 3.1. Account Authorization 3
- 3.2. How is access requested? 3
- 3.3. Who approves access? 3
- 3.4. How are credentials issued? 3
- 3.5. User Roles and Separation of Duties 4
- 3.6. Account Management 8
- 3.7. Forgotten Passwords / Account Lockout 8
- 4. Audit Log Review Process 9
- 5. Other iComplaints Security Settings 10
- 6. Document Maintenance 10

Record of Changes

Change Date	Version	Originator	Description Of Changes
09/25/2014	Final	FHFA IT Security	Initial document developed

1. Scope of this Document

This document identifies the procedures for granting, maintaining, and terminating access to the iComplaints system for FHFA users.

2. Introduction

MicroPact Engineering’s iComplaints is an enterprise level COTS (Commercial Off-The-Shelf) product that provides all of the functionality required to collect, track, manage, process, and report on information regarding EEO complaints and cases.

Users access the MicroPact Product Suite system via the Internet. All of the logic and processing functionality of MicroPact Product Suite resides on one or more central servers, with users accessing MicroPact Product Suite from their PC client Web browsers. On a network level, a user accesses the MicroPact Product Suite site (<https://FedRAMP.entellitrak.com/>) via the webserver using port 443.

While MicroPact is responsible for implementing technical and operational security controls for the system, FHFA is still required to ensure that the system is being operated in accordance with FHFA security policies and standards.

This document serves in place of an SSP to define FHFA’s implementation of account management controls (AC family) and audit and accountability controls (AU family) for the iComplaint system.

2.1. iComplaints FHFA Administrators

Role	Name	Phone	Email
iComplaints System Owner	Brian Guy	202-649-3019	Brian.guy@fhfa.gov
iComplaints Master Administrator	Evan Hall	202-649-3683	Evan.hall@fhfa.gov

3. Access Control Process

3.1. Account Authorization

iComplaints is accessed by FHFA employees and contractors who have been granted authorization by the FHFA system owner.

The system is accessed over the Internet at: <https://fhfa.icomplaints.com>

3.2. How is access requested?

Access can be granted to FHFA users with a legitimate business need to access the iComplaint system. Access request must be submitted in writing to the iComplaint system owner, or to the help desk.

3.3. Who approves access?

Access must be approved by the FHFA system owner.

3.4. How are credentials issued?

The system owner creates a new iComplaints user account by defining a username and password.

Passwords are not linked to FHFA user accounts, but they are forced to follow agency password complexity standards whereby they are:

- 12 Characters minimum
- One lowercase
- One alphanumeric
- No space
- Cannot re-use last 24 passwords.

The system owner shall pre-expire the password by enabling the “First Password Expiration Period” setting to “Immediately”. This will require the password to be changed by the user upon initial logon.

The system owner can then provide the new user their username and password via email.

3.5. User Roles and Separation of Duties

iComplaints has built in separation of duties controls in that no single role can maintain privileges from the “System Administration” family (i.e. Role Configuration, Password Configuration, etc.) as well as a “Case Processing Family.” However, users can be assigned multiple roles, but they can only perform actions from a single role at any given time, and must manually change roles in order to perform actions specific to a separate role.

The FHFA iComplaints system owner is permitted to add/remove system users. Therefore, they shall be assigned to the Administrator role as well as the Super Processor role, as defined below. The Master Administrator role shall be maintained by an OTIM employee, and this user is the only individual authorized to configure system security settings.

iComplaints users can be assigned any of four roles:

1. Master Administrator Role

The Master Administrator shall be occupied by a member of the Office of Technology and Information Management (OTIM). They shall have all permissions related to system administration and navigation, and shall be restricted from having any case processing, case navigation or case searching capabilities.

System Role Details

Role Name: [\[Select All\]](#) [\[Select None\]](#)

Role Status: [\[Select All\]](#) [\[Select None\]](#)

Note: At least one System privilege must be checked before this role can be saved.

User's Main Function

- Manage Cases
- Process Cases
- Administer System
 - Access Role Configuration
 - Access User Management
 - Set Password Expiration Policy
 - Access Reference Tables
 - Access Data Management
 - Access Reports
- System Navigation**
 - Generate User Reports
 - Manage Resources
 - Generate Mgmt Reports
 - DBA Access
 - Save DBA-SQL Query
 - Future Use
 - Search a Case

Case Processing Options

Assign/Reassign Case Options

- Assign Counselor
- Reassign Counselor
- Assign Manager
- Reassign Manager
- Assign Investigator
- Reassign To Parent Level Users

Create Case Options

- Create EEO Contact Cases
- Create Class Action Cases
- Create Pre-complaint Cases
- Create Mixed Cases
- Create Formal Cases

Convert Case Options

- Convert Pre-complaint to Formal
- Convert Formal to Mixed
- Convert Pre-complaint to Class
- Convert Mixed to Formal
- Convert Formal to Pre-complaint
- Convert Pre-complaint to Class
- Convert Pre-complaint to EEO Contact

Case Event Options

- Add Pre-complaint Event to Formal/Mixed/Class Case
- Add Events to Closed Pre-complaint
- Add Formal Event During Post Closure
- Edit Pre-complaint Events for Formal/Mixed/Class Cases
- Add Mixed Events During Post Closure
- Add Class Events During Post Closure

Class Case Options

- Certify Class Cases
- Search Class Candidates

Additional Case Options

- Delete a Case
- Consolidate Cases
- View All Cases
- Edit All Cases
- Email Case Details
- Edit UID Field
- Edit Hours

Case Navigation

- View Contacts Tab
- View Fees Tab
- View Hours Tab
- View Events Tab
- View Document Tab
- View Closure Tab
- View Claims Tab
- View Corrective Action Tab
- View ROI Tab

Search Options

- View Complaint Against for Searches
- View Complaint Against for No Fear and 462 Reports
- View Case Details for all Search Results
- View Pre-complaint Complaints
- View Formal Complaints
- View Mixed Complaints
- View Class Complaints
- View Complaint Against Pre-complaint Complaints
- View Complaint Against Formal Complaints
- View Complaint Against Mixed Complaints
- View Complaint Against Class Complaints

Other

- View OECMA
- View Complaint Against Activity
- EEO 462 Include Mixed Cases
- Log 462 Queries
- Log No Fear Queries

Figure 1: Master Administrator Permissions

2. Super Processor Role

The system owner will be assigned to the Super Processor role. The Super Processor will have full control over all iComplaints Case Processing data, and shall not maintain system administration functions maintained by the Master Administrator.

System Role Details

Role Name

Role Status

Note: At least one System privilege must be checked before this role can be saved.

Super Processor Function
 This role will enable a user to process and manage all the cases across your organization. It will also allow a user to perform a variety of actions, available within iComplaints, on all the cases. Only a few employees should be assigned this role to maintain the privacy and integrity of the data.

User's Main Function

- Manage Cases
- Process Cases
- Administer System
- Access Role Configuration
- Access User Management
- Set Password Expiration Policy
- Access Reference Tables
- Access Data Management
- Access Reports

System Navigation

- Generate User Reports
- Manage Resources
- Generate Mgmt Reports
- DBA Access
- Save DBA-SQL Query
- Future Use
- Search a Case

Case Processing Options

Assign/Reassign Case Options

- Assign Counselor
- Reassign Counselor
- Assign Manager
- Reassign Manager
- Assign Investigator
- Reassign To Parent Level Users

Create Case Options

- Create EEO Contact Cases
- Create Class Action Cases
- Create Pre-complaint Cases
- Create Mixed Cases
- Create Formal Cases

Convert Case Options

- Convert Pre-complaint to Formal
- Convert Formal to Mixed
- Convert Pre-complaint to Class
- Convert Pre-complaint to Mixed
- Convert Mixed to Formal
- Convert Formal to Pre-complaint
- Convert Pre-complaint to Class
- Convert Pre-complaint to EEO Contact

Case Event Options

- Add Pre-complaint Event to Formal/Mixed/Class Case
- Add Events to Closed Pre-complaint
- Add Formal Event During Post Closure
- Edit Pre-complaint Events for Formal/Mixed/Class Cases
- Add Mixed Events During Post Closure
- Add Class Events During Post Closure

Class Case Options

- Certify Class Cases
- Search Class Candidates

Additional Case Options

- Delete a Case
- Consolidate Cases
- View All Cases
- Edit All Cases
- Email Case Details
- Edit UID Field
- Edit Hours

Case Navigation

- View Contacts Tab
- View Fees Tab
- View Hours Tab
- View Events Tab
- View Document Tab
- View Closure Tab
- View Claims Tab
- View Corrective Action Tab
- View ROI Tab

Search Options

- View Complaint Against for Searches
- View Complaint Against for No Fear and 462 Reports
- View Case Details for all Search Results
- View Pre-complaint Complaints
- View Formal Complaints
- View Mixed Complaints
- View Class Complaints
- View Complaint Against Pre-complaint Complaints
- View Complaint Against Formal Complaints
- View Complaint Against Mixed Complaints
- View Complaint Against Class Complaints

Other

- View OECMA
- View Complaint Against Activity
- EEO 462 Include Mixed Cases
- Log 462 Queries
- Log No Fear Queries

Figure 2: Super Processor Permissions

3. Super User

Users assigned to the Super User role will have access similar to the Super Processor, with a limited scope, as defined by the system owner.

System Role Details

Role Name [\[Select All\]](#) [\[Select None\]](#)

Role Status [\[Select All\]](#) [\[Select None\]](#)

Note: At least one System privilege must be checked before this role can be saved.

User's Main Function

- Manage Cases
- Process Cases
- Administer System
- Access Role Configuration
- Access User Management
- Set Password Expiration Policy
- Access Reference Tables
- Access Data Management
- Access Reports

System Navigation

- Generate User Reports
- Manage Resources
- Generate Mgmt Reports
- DBA Access
- Save DBA-SQL Query
- Future Use
- Search a Case

Case Processing Options

Assign/Reassign Case Options

- Assign Counselor
- Reassign Counselor
- Assign Manager
- Reassign Manager
- Assign Investigator
- Reassign To Parent Level Users

Create Case Options

- Create EEO Contact Cases
- Create Class Action Cases
- Create Pre-complaint Cases
- Create Mixed Cases
- Create Formal Cases

Convert Case Options

- Convert Pre-complaint to Formal
- Convert Formal to Mixed
- Convert Pre-complaint to Class
- Convert Pre-complaint to Mixed
- Convert Mixed to Formal
- Convert Formal to Pre-complaint
- Convert Pre-complaint to Class
- Convert Pre-complaint to EEO Contact

Case Event Options

- Add Pre-complaint Event to Formal/Mixed/Class Case
- Add Events to Closed Pre-complaint
- Add Formal Event During Post Closure
- Edit Pre-complaint Events for Formal/Mixed/Class Cases
- Add Mixed Events During Post Closure
- Add Class Events During Post Closure

Class Case Options

- Certify Class Cases
- Search Class Candidates

Additional Case Options

- Delete a Case
- Consolidate Cases
- View All Cases
- Edit UID Field
- Edit Hours

Case Navigation

- View Contacts Tab
- View Fees Tab
- View Hours Tab
- View Events Tab
- View Document Tab
- View Closure Tab
- View Claims Tab
- View Corrective Action Tab
- View ROI Tab

Search Options

- View Complaint Against for Searches
- View Complaint Against for No Fear and 462 Reports
- View Case Details for all Search Results
- View Pre-complaint Complaints
- View Formal Complaints
- View Mixed Complaints
- View Class Complaints
- View Complaint Against Pre-complaint Complaints
- View Complaint Against Formal Complaints
- View Complaint Against Mixed Complaints
- View Complaint Against Class Complaints

Other

- View OECMA
- View Complaint Against Activity
- EEO 462 Include Mixed Cases
- Log 462 Queries
- Log No Fear Queries

Figure 3: Super User Permissions

4. Administrator

Users assigned to the administrator role will be able to add/delete iComplaints users, and view audit logs, but they will not have access to the global configuration settings such as role configuration and password settings, which will only be accessible by the Master Administrator.

Figure 4: Administrator Role Permissions

3.6. Account Management

At least annually, the iComplaints system owner shall print out the list of current FHFA users and their assigned role(s), and will review the list to determine if all users still need their current access, or if any accounts can be removed, or access reduced in accordance with the principle of least privilege.

The iComplaints system owner will mark any changes in access on the printed copy of the user list, and will sign and date a user authorization form provided by OTIM IT Security. The user list and authorization form will then be provided to OTIM IT Security for record. The iComplaints system owner will then implement the changes to the affected users.

3.7. Forgotten Passwords / Account Lockout

iComplaints passwords have been configured to expire every 60 days. The system will notify users, upon login, when their password is within 10 days of expiration.

iComplaints users can change their password at any time, or request a new password at the logon screen, which will be emailed to them.

Accounts are locked after three consecutive failed login attempts. The system owner or administrator must be contacted to unlock the account and reset the password.

4. Audit Log Review Process

Monthly, the system owner will review an audit log of user activity by first changing their role to “Administrator” and then selecting “Administration” → “Data Management” → “View Audit Log”.

MicroPact Internet Complaints System - Google Chrome
 fhfa-dev.icomplaints.com/icompl-fhfa-dev/jsp/home/admin/LogView.jsp

icomplaints
 MicroPact iComplaints System Session will expire in 30 minutes Wed Sep 24 16:34:58 EDT 2014

Log Viewer

Please enter your search criteria below.

Filter by User Like

Sort by Date / Time In Descending order

<< View Log Record >>

Number of rows to display per page: 50

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ... Next 15
 viewing 1 - 50 of 336921

View Audit Log

User ID	User	Action	Description	Complaint ID	IP Address	Date / Time
78	Evhall	LOGIN PASS	Successful login.		12.183.70.2	2014-09-24 16:34:45.847
78	Evhall	ADMIN UPDATED USER PROFILE	Update user profile 'Evhall(78)'		12.183.70.2	2014-09-24 16:29:40.543
78	Evhall	LOGIN PASS	Successful login.		12.183.70.2	2014-09-24 16:25:39.227
78	Evhall	LOGOUT	Log out of system.		12.183.70.2	2014-09-24 16:24:33.86
78	Evhall	USER REMOVED	User deleted flag set with userid = 72		12.183.70.2	2014-09-24 16:23:41.31
78	Evhall	USER SWITCHED ROLE	User switched role to Master Administrator		12.183.70.2	2014-09-24 16:22:58.39
78	Evhall	UPDATED USER PROFILE	Update user profile		12.183.70.2	2014-09-24 16:22:58.347
78	Evhall	USER SWITCHED ROLE	User switched role to Super Processor		12.183.70.2	2014-09-24 16:22:53.477
78	Evhall	UPDATED USER PROFILE	Update user profile		12.183.70.2	2014-09-24 16:22:53.433
78	Evhall	LOGIN PASS	Successful login.		12.183.70.2	2014-09-24 16:22:47.427
79	brianguy	LOGOUT	Log out of system.		12.183.70.2	2014-09-24 16:22:31.54
79	brianguy	LOGIN PASS	Successful login.		12.183.70.2	2014-09-24 16:22:20.29
78	Evhall	LOGOUT	Log out of system.		12.183.70.2	2014-09-24 16:22:14.973
78	Evhall	ADMIN UPDATED USER ROLE	Click To Display Description		12.183.70.2	2014-09-24 16:21:46.65
78	Evhall	ADMIN UPDATED USER PROFILE	Update user profile 'brianguy(79)'		12.183.70.2	2014-09-24 16:21:46.647
1	Administrator	LOGOUT	Log out of system.		216.54.171.18	2014-09-24 16:19:56.09
1	Administrator	ADMIN UPDATED USER ROLE	Click To Display Description		216.54.171.18	2014-09-24 16:19:49.11
1	Administrator	ADMIN UPDATED USER PROFILE	Update user profile 'microtest(65)'		216.54.171.18	2014-09-24 16:19:49.107

The system owner will send an email to #AuditLogReview, stating that the audit log has been reviewed, and noting in the email if any suspicious activity was identified, or not.

If any suspicious activity was identified (privilege escalation attempts, users performing unauthorized actions), the system owner will notify IOITMSecurity@fhfa.gov.

5. Other iComplaints Security Settings

iComplaint user sessions expire after 30 minutes of inactivity. A warning is presented to the user 5 minutes prior to the end of the session.

User accounts will be disabled if they have not been logged into for 60 days.

6. Document Maintenance

The iComplaints system owner will be responsible for updating this procedure whenever changes occur.