

Enterprise Income Verification (EIV 9.9a) System

Multifamily Housing Programs

Security Administration Manual

U.S. Department of Housing and Urban Development

October 2016

Revision History

Version	Date	Comments required	Approvals required
Version 1.0	09/16/05	Build 4.0 Release	
Version 2.0	03/10/06	Build 5.0 Release	
Version 3.0	08/17/06	Build 6.0 Release	
Version 4.0	04/18/2007	Build 7.0 Release	
Version 5.0	10/30/2007	Build 8.0 Release	
Version 6.0	04/01/2008	Build 8.1 Release	
Version 6.1	04/25/2008	Updated based on review comments	
Version 6.2	04/30/2008	Updated the manual to include only PIH information. MF EIV security administration will be a separate document	
Version 7.0	09/08/2009	Updated the manual for Release 9.0	
Version 7.1	09/09/2009	Updated the screen shots based on MF Program area comments	
Version 8.0	04/04/2010	Build 9.1 Release	
Version 9.0	10/26/2011	Build 9.2.1 Release	
Version 10.0	03/14/2012	Minor Updates for Build 9.3 Release	
Version 10.1	06/01/2012	Updated based on comments received from MF Program Area	
Version 10.2	04/22/2013	Minor Updates for Build 9.5 Release	
Version 11	05/18/2014	Minor Updates for Build 9.7 Release	
Version 12	12/19/2014	Minor Updates for Build 9.8 Release	
Version 13	05/27/2015	Minor Updates for Build 9.9 Release	
Version 14	06/08/2016	Updated the Privacy Act and Security Awareness Training links	
Version 15	10/11/2016	Updated Security Awareness link and instructions	



Enterprise Income Verification – Security Administration Manual Authorization Memorandum

I have carefully assessed the Security Administration Manual for the Enterprise Income Verification (EIV) system. This document has been completed in accordance with the requirements of the HUD System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

Metzy Martinez
EIV IT Project Manager

Date

Danielle D. Garcia
Branch Chief, Subsidy Oversight

Date

John J. Curry Jr.
Housing Program Manager,
Office of Program Systems Management

Date

Table of Contents

1	PREFACE	1-1
1.1	Document Overview	1-2
2	INTRODUCTION	2-1
2.1	System Overview	2-2
2.2	Contingencies and Alternate Modes of Operation	2-3
2.3	Security	2-3
2.3.1	User Accounts	2-4
2.3.2	Security Awareness	2-4
2.3.3	Protecting Privacy Act Information	2-5
2.3.4	Shifting Between EIV and other WASS Systems.....	2-5
2.3.5	If the User Needs to Leave His or Her Work Desk.....	2-6
2.3.6	When the User Has Finished the EIV Work Session	2-6
2.3.7	Audits and User Activity Logging.....	2-7
2.3.8	Standard Features	2-7
3	MULTIFAMILY HOUSING SECURITY ADMINISTRATORS	3-1
3.1	Audit Reports.....	3-2
3.2	User Session and Activity Audit Report	3-2
3.3	Tenant Data Access Audit Report.....	3-3
4	RESPONSIBILITIES OF EIV SECURITY ADMINISTRATORS	4-1
4.1	Purpose of Reports	4-2
4.2	Role of the EIV Security Administrator	4-2
4.3	The Need to Avoid Conflict of Interest	4-2
	APPENDIX A - ABBREVIATIONS AND ACRONYMS.....	A-1

List of Figures

Figure 1 - EIV data flow/system interfaces.....	2-3
---	-----



1 Preface

1 Preface

1.1 Document Overview

The purpose of this manual is to provide guidance to Multifamily Housing Programs (Multifamily Housing) personnel responsible for security administration in the Enterprise Income Verification (EIV) application on security concerns and responsibilities. The manual details business operational procedures for successfully performing administration tasks using reports available in EIV and interfacing with other program office and CIO personnel responsible for security.

The Office of Public and Indian Housing (PIH) also uses the EIV system and there is an interface between Multifamily Housing and PIH in both the Existing Tenant Search and Multiple Subsidy Search which are found in the EIV system. This manual only addresses Multifamily Housing.

1.1.1 How This Manual Is Organized

Listed below are each of the chapters contained in this manual, along with a brief description of its content:

- **Chapter 2, Introduction** – An overview of EIV, including the hardware, software, and system architecture.
- **Chapter 3, Multifamily Housing Security Administrators** – Provides instruction on the functions available to Multifamily Housing Security Administrators.
- **Chapter 4, Responsibilities of EIV Security Administrators** - Provides an overview of the EIV Security Administrators responsibilities in protecting the integrity of the system.
- **Appendix A, Abbreviations and Acronyms** – Provides a list of commonly used abbreviations and acronyms.

1.1.2 Who Should Use This Manual?

This manual is intended for the following users:

- Multifamily Housing users with HQ User Administrator (HQA) role defined in WASS
- Multifamily Housing users with HQ Security Administrator (HQS) role defined in WASS
- Multifamily Housing users with Help Desk (HDK) role defined in WASS

If you have other roles or other action codes, you may need to access other documents in the EIV library to learn more about them. For more information about the content of the EIV library, refer below to Section 1.1.3, *Related Documentation* section of this document.

This manual assumes the resources assigned to these roles have the following knowledge or expertise:

- Working knowledge of Microsoft Windows.

- Operational understanding of PCs.
- Operational understanding of Internet browsers.
- Understanding of basic network concepts.
- Understanding of HUD program terminology, policies, and procedures.

1.1.3 Related Documentation

This section provides a list of related documents in the EIV library:

- *EIV User Manual – For Multifamily Housing Users* – For Multifamily Housing users, this manual provides step-by-step instructions. Users should be familiar with PCs, Microsoft Windows, and their browser software.
- *EIV Multifamily User Administration Manuals* (internal and external) – For Multifamily Housing user administrators (internal and external user administrators), these manuals provide step-by-step instructions on user administration functions available in WASS and EIV.

2 Introduction

2 Introduction

EIV provides a portal to tenant income information in the form of household income data, as well as several income-based reports. EIV is a Web-based system, allowing access to information across secure Internet connections to the HUD application server using Microsoft Internet Explorer Version 6.0 or higher.

2.1 System Overview

The Office of Multifamily Housing tenant income and benefits data in the EIV system come from a variety of sources:

1. **WASS** – serves as the single sign-on portal used by EIV and other HUD systems. It also is used for EIV Office of Multifamily Housing role assignment.
2. **IMS (formerly PIC) Form HUD-50058 Database** – provides PIH tenant information and related data originating from form HUD – 50058. This information is displayed in the Existing Tenant Search and Multiple Subsidy Report modules.
3. **TRACS Form HUD-50059 Database** – provides Multifamily Housing tenant information originating from form HUD-50059.
4. **NDNH** – provides data including wages, unemployment insurance income, and W-4 (“new hires”) data reported by State and Federal Agencies to the HHS/Office of Child Support Enforcement (OCSE) through matching Multifamily Housing tenant ID information against NDNH databases.
5. **SSA** – provides benefit information including disability, supplemental income, and Social Security payments through matching Multifamily Housing tenant ID information against SSA databases.

Data exchange with the Social Security Administration (SSA) for Social Security and Supplemental Security Income benefits data follows a quarterly cycle with approximately one-third of tenants being matched each month (according to their re-certification month) with new tenants added in for the first available match cycle.

Data exchange with the HHS National Directory of New Hires (NDNH) databases also follows a quarterly cycle for wages and unemployment benefits data but W-4 data are updated monthly and all data is collected monthly for new MF tenants, and household members who turn 18 (no data is collected from NDNH concerning those under 18).

Introduction

Figure 1 below illustrates the EIV data flow/system interfaces.

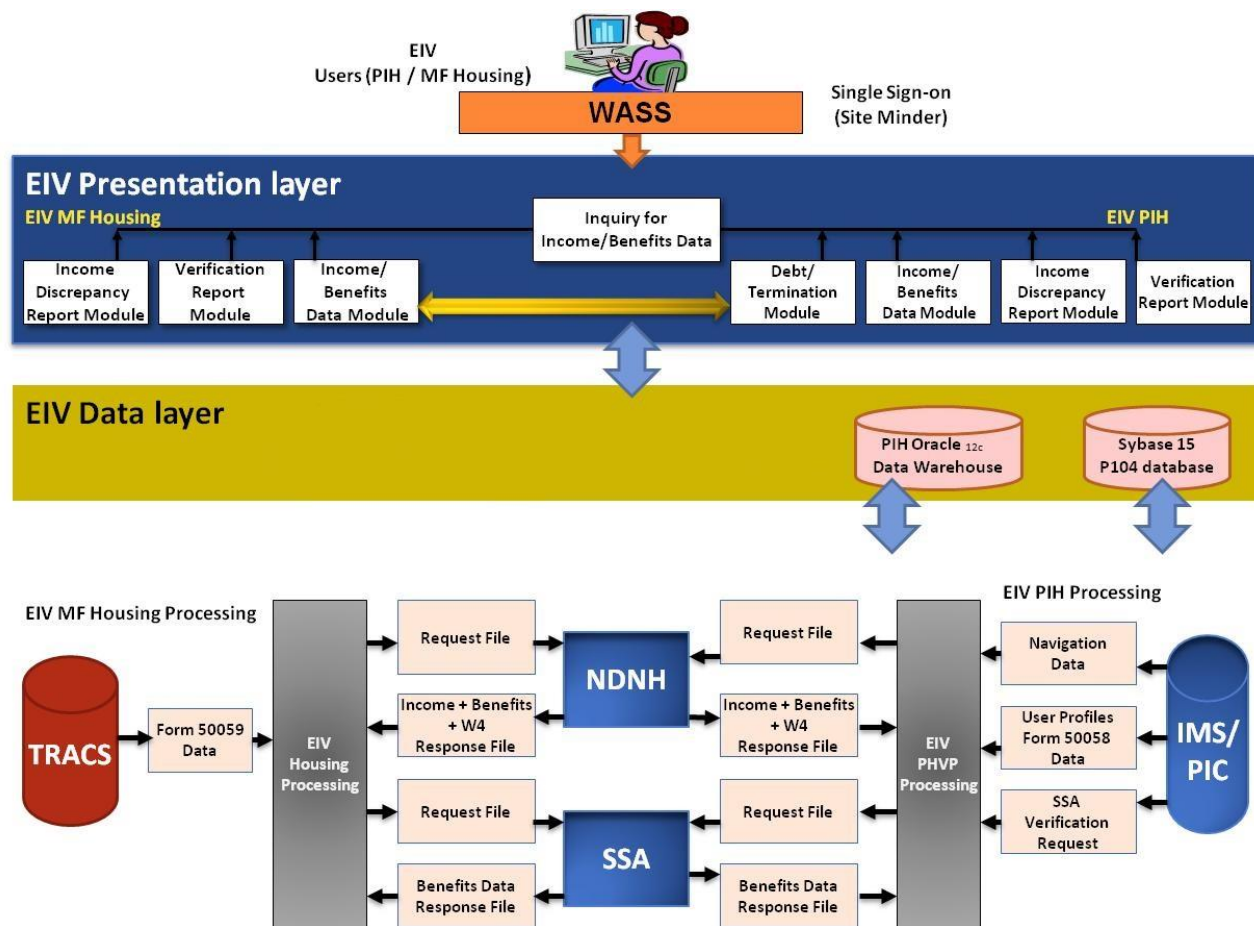


Figure 1 - EIV data flow/system interfaces

2.2 Contingencies and Alternate Modes of Operation

EIV operates 24 hours a day, 7 days per week (except on the first weekend of each month when IMS/PIC summarization processing makes heavy use of the shared database). However, the best conditions for use are during weekdays because EIV batch processing runs over night and during weekends, which may impact system responsiveness and files that are in the process of being updated may have incomplete data. **Notices of planned outages for system maintenance will be posted in the Announcement Area inside EIV.** Guidance and reference material may be found in the Multifamily Housing EIV web page and on the EIV system welcome page:

<http://www.hud.gov/offices/hsg/mfh/rhiip/eiv/eivhome.cfm>

2.3 Security

EIV contains personal information concerning tenants covered by the Privacy Act, such as wage and income data, as well as identifying information such as Social Security Number, address, and employment information. This information may only be used for limited official purposes, which are tenant recertification and oversight of the tenant recertification process (which includes use by the

Introduction

Office of Inspector General (OIG) and the Government Accountability Office (GAO)). It does not include sharing with governmental entities not involved in the recertification process. Users are encouraged to refer any non-standard requests for access to HUD management and to report any unauthorized disclosure of EIV data to the HUD Privacy Act Officer or to the OIG. If it appears that the system has been “hacked”, that should be reported to the HUD Help Desk (1-888-297-8689).

All EIV users must adhere to the EIV Rules of Behavior. A copy of the Rules of Behavior is incorporated in the Coordinator Access Authorization Form (CAAF) and the User Access Authorization Form (UAAF) which are the forms that must be signed and used for applying for access to the EIV system. A copy of each form is posted on the Multifamily Housing EIV web page, cited above. The rules clearly delineate responsibilities of, and expectations for, all individuals with access to the EIV system. Non-compliance with these rules will be disciplined through sanctions commensurate with the level of infraction. Sanctions against HUD staff may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination depending on the severity of the violation. Sanctions against HUD contractors may range from removal of system access for a specific period of time or indefinitely. Sanctions against HUD business partners may range from removal of system access for a specific period of time or indefinitely or if the violation is significant or persistent, the HUD business partner itself may lose access. Privacy Act violations may result in civil or criminal prosecution.

Access to tenant data is logged as part of the effort to protect the data and provide traceability should a questionable event occurs. Printouts of reports containing tenant personal information display the name and partial HUD (WASS) ID of the requestor on each page.

2.3.1 User Accounts

User accounts for the EIV system should be provided on a need-to-know basis, with appropriate approval and authorization. EIV User Administrators with the HDK role are to maintain a file for each EIV Coordinator with the access authorizations signed by the responsible manager and the EIV User Agreement signed by the Coordinator, which includes the EIV Rules of Behavior. User Administrators with the HDK role are required to certify annually that EIV Coordinators have appropriate rights in EIV. User accounts that have not been certified within 30 days thereafter will lose their EIV roles and will not be able to access EIV or to certify their users. User Administrators need to be able to confirm that the Coordinator roles need to be continued before making the certification.

2.3.2 Security Awareness

New EIV system users are to receive as part of their training a familiarization with the requirements of the Privacy Act. Users are required to have annual online Federal Information Systems Security (ISS) Awareness training to refresh and update that initial training. Potential EIV users must sign the EIV Access Request (Coordinator Access Authorization Form or User Access Authorization Form) to signify that they understand and accept the EIV Rules of Behavior. The CAAF and UAAF can be obtained at:

http://portal.hud.gov/hudportal/HUD?src=/program_offices/housing/mfh/rhiip/eiv/eivapps

The complete text of the Privacy Act is available at <https://www.justice.gov/opcl/privacy-act-1974>

To meet this requirement, EIV users must complete the online ISS Awareness training program. Federal Employees are to utilize the DoD Employee course version, *CyberAwareness Challenge Department of*

Introduction

Defense Version. At the end of the training, EIV users must print and maintain the Certificate of Completion provided.

To complete online Security Awareness Training:

Step 1: Open your web browser

Step 2: Type http://iatraining.disa.mil/eta/cyberchallenge_v4/launchPage.htm into the URL box and press **Enter**

Step 3: Under Department of Defense Employees header select the appropriate link, **Start/Continue Cyber Awareness Challenge** or **Retake Cyber Awareness Challenge**.

When the training is complete, print and maintain the Certificate of Completion.

Note: The Security Awareness Training described above is the same training required for those individuals who transmit TRACS files. If the training has been completed to satisfy TRACS security training requirements, this will also satisfy EIV security training requirements as well provided the completion date represented on the Certificate of Completion is not older than one year.

2.3.3 Protecting Privacy Act Information

Because EIV contains personal information protected by the Privacy Act, it is extremely important that users avoid leaving the system, printouts or downloads containing personal information unattended at their desks or where they may be seen by visitors. If someone is done working using EIV for the day or will not need it for a while, the best practice is to close the browser window and either file or shred any printed output containing personal information. Disks or other electronic media containing downloaded personal information are to be stored away when not in use and destroyed when no longer needed.

The easiest way to distinguish printed output containing Privacy Act information from summary reports is that the printouts containing Privacy Act information have the Privacy Act warning at the bottom of each page. In addition, personal information should never be placed in the body of an e-mail message. It may only be sent in an attached file that has been encrypted using software that meets National Institute of Standards and Technologies FIPS 140-2 encryption standards. HUD has installed McAfee Endpoint Encryption on its laptops and plans to install it on HUD PC's. That software encrypts the hard disk and all files on it. PKZip12, also used by HUD, has a file encryption option. However, that encryption option works only one file at a time rather than the whole hard disk. Both meet the FIPS 140-2 standard. Information and additional guidance regarding the use of encryption software may be found at the HUD Computer Self-Help Desk

<http://hudsharepoint.hud.gov/sites/apps/CSHD/SitePages/Home.aspx> .

It should be kept in mind that TRACS and IMS/PIC also contain personal information protected by the Privacy Act, so the same rules and practices apply.

2.3.4 Shifting Between EIV and other WASS Systems

If a user needs to exit EIV to work in another WASS system such as TRACS, they should click on the Back to Secure Systems link to log out of EIV as shown below. This will bring them back to the WASS Main Menu from which they may access other WASS systems to which they have been granted access. When they are done working in another system, from the WASS main menu, they should click on the Enterprise Income Verification (EIV) link and a new session of EIV will be opened.

2.3.5 If the User Needs to Leave His or Her Work Desk

Users should never leave their PC unattended with either EIV or WASS active. If WASS is active, someone can reenter EIV or access another WASS system to which the user has access merely by clicking on the WASS link. If the user intends to return to EIV or another system accessed through WASS, they should activate a screen saver while away from their desk. The same is true if they have visitors. However, if they do not return within 30 minutes, their sessions on EIV and to WASS will have timed out.

2.3.6 When the User Has Finished the EIV Work Session

When users are done working in EIV, and if they do not intend to work in another WASS system, it is important to exit both EIV and WASS by closing the browser. This may be accomplished by clicking on Back to Secure Systems from the top of the left-side menu and, once at the Secure Systems page, clicking on the Logout button and then clicking on OK. However, it is far simpler to close the browser window by clicking on the “X” in the upper-right-hand of the browser window. This may be done from within EIV.

Enterprise Income Verification HUD Home MF Housing EIV Home Search Email

Welcome FIRST - HEIV01 LAST - uiv

EIV Announcements EIV v9.2.1.0

Announcement Date: 05/09/2011

As of May 9, 2011, the following PIH EIV reports are not available: Deceased Tenants, Identity Verification, Immigration, Multiple Subsidy, and Income Reports By Reexamination Month. These reports are scheduled to be available on Monday, May 16, 2011, upon successful completion of the weekend summarization job. We apologize for the inconvenience.

PIH Training Announcement

PIH is pleased to offer **Updated** Enterprise Income Verification (EIV) System 9.2 training via webcast for all PIH EIV system users. Watch this webcast, which aired on May 2, 2011, at: <http://portal.hud.gov/hudportal/HUD?src=/press/multimedia/videos>.

Timeout Notice!

Your EIV Session will time out after thirty (30) minutes of inactivity, closing the session and logging you off the system. The page that was active at the time the session timed out will continue to display. Before you can perform another system function, after a time out occurs, you will be prompted to log on again.

Notice of Browser Compatibility

The EIV System supports browser version Internet Explorer 6.0 and higher. Other browsers may not be compatible with this software.

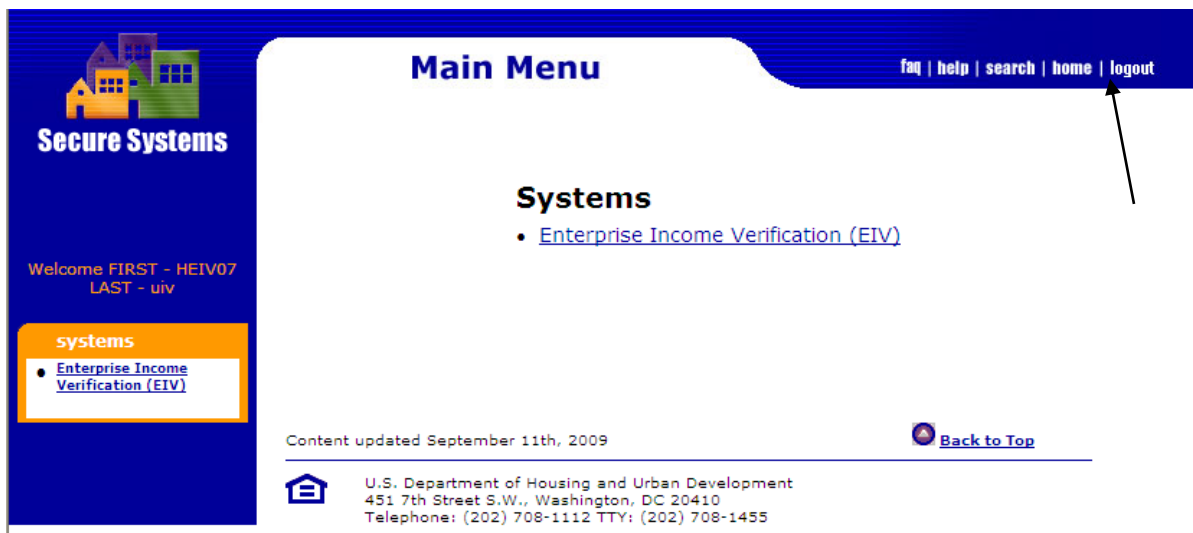
Attention !!

The Next User re-certification is due 6 months from your last certification date. Your certification period is semi-annual.

Navigation Menu:

- Back to Secure Systems
- Back to EIV Main Page
- Income Information**
 - By Contract Number
 - By Project Number
 - By Head of Household
- HQs Management Reports**
 - Certified Contracts/Projects
 - Usage/Terminations Summary
 - Income Discrepancy Summary
 - Verification Reports Summary
- Verification Reports**
 - Existing Tenant Search
 - Multiple Subsidy Report
 - Identity Verification Reports
 - Deceased Tenants Report
- User Administration**
 - User Certification
 - User Certification Report
 - User Maintenance
 - User Expiration Report
 - Coordinator User Report
- Audit Reports**
 - User Session & Activity
 - Tenant Data Access
- External Links**
 - USCIS - SAVE System

User Manual
Adobe Acrobat Reader



Guidance concerning security practices, governing the work area and storage of paper records containing personal information and their destruction when they no longer are needed, may be found at the Multifamily Housing EIV Web site.

2.3.7 Audits and User Activity Logging

Users of EIV are on notice that their activities and particularly tenant data access activities within the system and user administration transactions are logged for security audit and reporting purposes. These reports will include records of successful access of sensitive data to which the user is authorized. It is the responsibility of the EIV Security Administrator to review logs regularly and reports (daily if possible) to identify suspicious patterns of behavior or to research patterns of behavior where suspicious behavior has occurred.

Changes to the user roles and user certification transactions are also logged.

2.3.8 Standard Features

EIV provides the following standard features for security administrator functions:

Pagination

The reports available to EIV Security Administrators are displayed in groups of 50 records (e.g., households, users) per page. Where there are more than 50 records in the search results, the EIV system has links to the other groups of 50 records through links. Navigation to next group of pages, previous group of pages, first page and last page of the search results are also provided to allow the user to access different sets of search results.

Required Fields

Security Administration reports are generated based on the selection criteria fields. Fields marked with an asterisk (*) are the fields required in order to generate the report.

3 Multifamily Housing Security Administrators

3 Multifamily Housing Security Administrators

The next sub-sections provide instructions on the EIV functions available to Multifamily Housing Security Administrators.

3.1 Audit Reports

Audit reports allow the Office of Multifamily Housing Security Administrator to generate and review reports summarizing system and data use.

The following reports are discussed in this chapter:

- [User Session and Activity Audit Report](#)
- [Tenant Data Access Audit Report](#)

3.2 User Session and Activity Audit Report


This report details each user session and the pages accessed during the session. To view the User Session and Activity audit report, complete the following steps:

- Click the [User Session and Activity](#) link available to Multifamily Housing program users.

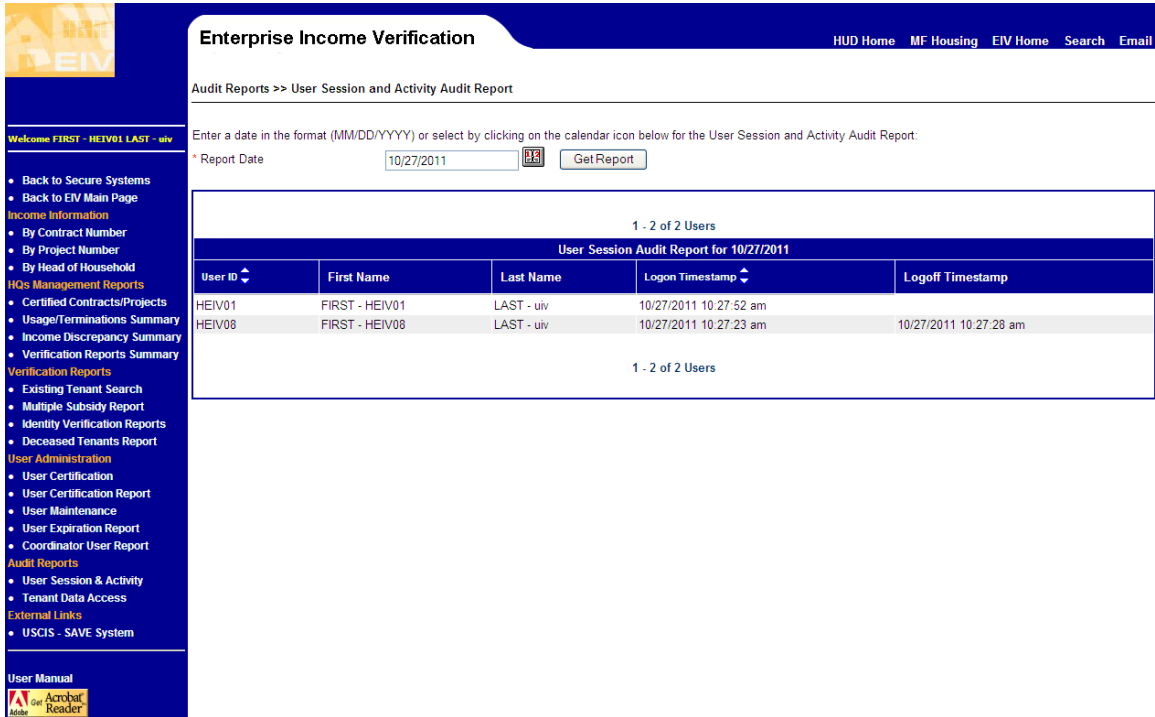
The system displays the **User Session and Activity Audit Report** page as shown below.

The screenshot displays the EIV system interface. The top navigation bar includes "Enterprise Income Verification" and links for "HUD Home", "MF Housing", "EIV Home", "Search", and "Email". The main content area shows the breadcrumb "Audit Reports >> User Session and Activity Audit Report". Below this, there is a text prompt: "Enter a date in the format (MM/DD/YYYY) or select by clicking on the calendar icon below for the User Session and Activity Audit Report:". A form field labeled "Report Date" contains a calendar icon and a "Get Report" button. On the left side, a vertical navigation menu lists various report categories, including "Income Information", "HQs Management Reports", "Verification Reports", "User Administration", "Audit Reports", and "External Links". An arrow points to the "User Session & Activity" link under the "Audit Reports" section. At the bottom left, there is a "User Manual" link and an Adobe Acrobat Reader icon.

Multifamily Housing Security Administrators

- Enter the **Report Date** in the format (MM/DD/YYYY), or select a date by clicking on the calendar () tool.
- Click **Get Report**.

The system displays the **User Session and Activity Audit Report** results page as shown below.



The screenshot shows the 'Enterprise Income Verification' interface. The page title is 'Enterprise Income Verification' and the breadcrumb is 'HUD Home > MF Housing > EIV Home > Search > Email'. The main heading is 'Audit Reports >> User Session and Activity Audit Report'. Below this, there is a form to enter a report date, with '10/27/2011' entered and a 'Get Report' button. The report results are displayed in a table titled 'User Session Audit Report for 10/27/2011'. The table has five columns: 'User ID', 'First Name', 'Last Name', 'Logon Timestamp', and 'Logoff Timestamp'. Two users are listed: HEIV01 and HEIV08. The left sidebar contains a navigation menu with categories like 'Income Information', 'HQs Management Reports', 'Verification Reports', 'User Administration', 'Audit Reports', and 'External Links'. At the bottom, there is a 'User Manual' link and an 'Acrobat Reader' icon.

1 - 2 of 2 Users				
User Session Audit Report for 10/27/2011				
User ID	First Name	Last Name	Logon Timestamp	Logoff Timestamp
HEIV01	FIRST - HEIV01	LAST - uiv	10/27/2011 10:27:52 am	
HEIV08	FIRST - HEIV08	LAST - uiv	10/27/2011 10:27:23 am	10/27/2011 10:27:28 am

3.3 Tenant Data Access Audit Report

This report provides a list of all EIV system users who have accessed the tenant wage and income data within a specified date range.

To view the Tenant Access Audit Report, complete the following steps:

- Click the [Tenant Data Access](#) link available to Multifamily Housing Users.

The system displays the **Tenant Data Access Audit Report** page as shown below:

Enterprise Income Verification HUD Home MF Housing EIV Home Search Email

Audit Reports >> [Tenant Data Access](#)

Specify the inclusive start and end dates for the time period and the User ID. You can also enter either Last Name or SSN of a tenant. Specify dates in the format (MM/DD/YYYY) or select by clicking on the calendar tool.

Required Fields

* Start Date

* End Date

Tenant SSN (XXX-XX-XXXX)

Tenant Last Name

* User ID

←

- Enter **Start Date** in the format (MM/DD/YYYY), or select one by clicking on the calendar tool. The Start Date defines the beginning date for the reporting period. The Start Date value cannot be greater than the End Date value.
- Enter **End Date** in the format (MM/DD/YYYY), or select one by clicking on the calendar tool. The End Date defines the ending date for the reporting period. The End Date value must be greater than the Start Date value. Please note that the **Start Date** and **End Date** range should not exceed **30 days**.
- Enter the **Tenant SSN** when you want to limit report content to a specific Social Security Number. This is an optional field.
- Enter the **Tenant Last Name** when you want to limit report content to a specific tenant's name. This is an optional field.
- Enter the **User ID** when you want to limit the report content by a specific user. This is an optional field.
- Click the **Get Report** button.

The system displays the **Tenant Data Access Audit Report** page as shown below:

Multifamily Housing Security Administrators

Enterprise Income Verification HUD Home MF Housing EIV Home Search Email

Audit Reports >> [Tenant Data Access](#)

Specify the inclusive start and end dates for the time period and the User ID. You can also enter either Last Name or SSN of a tenant. Specify dates in the format (MM/DD/YYYY) or select by clicking on the calendar tool.

Required Fields

* Start Date

* End Date

Tenant SSN (XXX-XX-XXXX)

Tenant Last Name

* User ID

1 - 1 of 1 Users

User ID	User Name	Date	SSN	Tenant Name	Re-certification Month	Subsidy Contract	Project Number
HEIV01	FIRST - HEIV01 LAST - uiv	2011-10-27 10:33:51.0	***-**-1895	MTTMIZSVZMUJ B BBINYV	N/A	AL0	

1 - 1 of 1 Users

Confidential. Privacy Act data. Civil and criminal penalties apply to misuse of this data.

Navigation Menu:

- Welcome **FIRST - HEIV01 LAST - uiv**
- Back to Secure Systems
- Back to EIV Main Page
- Income Information**
 - By Contract Number
 - By Project Number
 - By Head of Household
- HQs Management Reports**
 - Certified Contracts/Projects
 - Usage/Terminations Summary
 - Income Discrepancy Summary
 - Verification Reports Summary
- Verification Reports**
 - Existing Tenant Search
 - Multiple Subsidy Report
 - Identity Verification Reports
 - Deceased Tenants Report
- User Administration**
 - User Certification
 - User Certification Report
 - User Maintenance
 - User Expiration Report
 - Coordinator User Report
- Audit Reports**
 - User Session & Activity
 - Tenant Data Access
- External Links**
 - USCIS - SAVE System
- User Manual**

The following fields are displayed on the report:

- User ID - the assigned access ID for a user
- User Name - the user's first and last name
- Date - the date and time the access was made
- Tenant Name - the tenant's name that was accessed
- SSN – the tenant's SSN that was accessed
- Recertification Month - the Recertification Month selected when searching for Income Information – By Recertification Month
- Contract Number – the Contract Number associated to the household (Subsidy Contract in screenshot)
- Project Number - the Project Number associated to the household

4 Responsibilities of EIV Security Administrators

4 Responsibilities of EIV Security Administrators

The responsibility of EIV Security Administrators is to protect the integrity of the system.

4.1 Purpose of Reports

The purpose of the reports that are available to EIV Security Administrators is to help them identify if there may be a situation wherein a user is abusing his/her system access to use the information for private purposes, perhaps to misuse identify information or to sell it.

4.2 Role of the EIV Security Administrator

EIV Security Administrators are not expected to be investigators or to make accusations. If there is reason to think that the EIV system is being abused, that access to information is being used for improper purposes, to protect the integrity of system, the Security Administrator should report the facts to the OIG. If the facts are not clear, the EIV Security Administrators may consult with counterparts, the Headquarters EIV Security Administrator, or experts in the Headquarters program office and then report the facts to the OIG if appropriate. Failure of a HUD office or Owner/Agent to follow proper security practices to protect personal information covered by the Privacy Act should be reported to the Office of Asset Management and Portfolio Oversight (OAMPO), Subsidy Oversight Division . This may result in suspension of EIV access. Improper disclosure of personal information covered by the Privacy Act should be reported to the HUD Privacy Act Officer or OIG.

4.3 The Need to Avoid Conflict of Interest

Guidance from the National Institute of Standards and Technology, which sets Federal security standards, is that security personnel should avoid serving in other roles for the same system. The purpose of that guidance is to help assure that security personnel do not have a conflict of interest in being responsible for performing the very functions that they may monitor. This is particularly a potential problem in serving as both EIV User Administrator and EIV Security Administrator. That is because while EIV generally is not a transactional system, the User Administrators are ones who perform transactions in EIV. EIV Security Administrators are responsible for monitoring those same transactions.

APPENDIX A – ABBREVIATIONS AND ACRONYMS

The following abbreviations and acronyms may or may not appear in this document. They are provided for reference and clarity.

Acronym	Definition
C&A	Certification and Accreditation
CAAF	Coordinator Access Authorization Form
CAN	Claim Account Number
CCB	Change Control Board
CCMB	Configuration Change Management Board
CIO	Chief Information Officer
CM	Configuration Management
CMRB	Contract Management Review Board
COTR	Contracting Officer's Technical Representative
DCG	Development Coordination Group
DRP	Disaster Recovery Plan
DTS	Data Transmission Services
EDI	Electronic Data Interchange
EIV	Enterprise Income Verification
FEIN	Federal Employer Identification Number
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FO	Field Office
FOIA	Freedom of Information Act
Form HUD-50058	Form used to submit resident characteristics and tenant income data to HUD for Office of Public and Indian Housing's programs
Form HUD-50059	Form used to submit resident characteristics and tenant income data to HUD for Office of Housing's programs
FOUO	For Official Use Only
FTP	File Transfer Protocol
GAO	Government Accountability Office
GTM	Government Technical Monitor
GTR	Government Technical Representative
HHS	U.S. Department of Health and Human Services
HOH	Head of Household
HOUSING	HUD's Office of Housing – FHA
Hub	Not an acronym. FO is classified into two categories – Hub and Program Center. A Hub can be a stand-alone FO or have another office, a Program Center, report to it.
HUD	US Department of Housing and Urban Development
ICN	Income Control Number
IMS	Inventory Management System (formerly PIC)
MF	Multifamily Housing
MOA/U	Memorandum of Agreement / Understanding
MTW	Moving To Work
NDNH	National Directory of New Hires

Acronym	Definition
NIST	National Institute of Standards and Technology
OCSE	Office of Child Support Enforcement
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPC	Office of Procurement & Contracts
PD&R	HUD's Office of Policy, Development and Research
PHA	Public Housing Authorities
PHVP	Public Housing and Voucher Programs
PI	Period of Income
PIA	Privacy Impact Assessment
PIC	Public & Indian Housing Information System (now IMS)
PIH	HUD's Office of Public & Indian Housing
POA&M	Plan of Action and Milestones
PVCS	Project Version Control System
PWS	Performance Work Statement
QA	Quality Assurance
QU	Quarterly Update
QW	Quarterly Wage
RHIIP	Rental Housing Integrity Improvement Project
RIM	Rental Integrity Monitoring
SEIN	State Employment Identification Number
SPH	HUD's Security Program Handbook
SPP	Security Program Policy
SS	Social Security
SSA	Social Security Administration
SSAA	System Security Authorization Agreement
SSI	Supplemental Security Income
SSO	Single Sign On (used in WASS)
SSP	System Security Plan
TARC	Troubled Agency Recovery Center
TASS	Tenant Assessment Subsystem
TRACS	Tenant Rental Assistance Certification System
TTP	Total Tenant Payment
UAAF	User Access Authorization Form
V V&T	Verification, Validation, & Test
W-4	New Hires data
WASS	Web Access Security Subsystem