Hobson City Apartments

Multifamily Subsidy

Enterprise Income Verification (EIV) System

Policy and Procedures

OFFICE COPY

UPDATE: 04/2026

Housing Opportunities Through Modernization Act of 2016

PURPOSE OF THE POLICY

The purpose of this policy is to provide instruction and information to staff, auditors, consultants, contractors and residents of Hobson City Apartments, on the acceptable use, disposition and storage of data obtained through the Enterprise Income Verification System.

The purpose of EIV is to assist the HUD Contract Administrators, owners, and their agents in streamlining the income verification process and to help in minimizing the need for third-party verification. EIV allows the user to identify:

- Applicants currently receiving HUD assistance
- Income not previously reported
- New employment
- Historical patterns of earnings and received income
- Multi-subsidy for household members included in both PIC and TRACS databases
- Deceased household members

In addition, information in EIV can be used to provide more comprehensive oversight to compliance policies and their implementation. The data provided via EIV system will be protected to ensure that it is only used for official purposes and not disclosed in any way that would violate the privacy of the individuals represented in the system data. Privacy of data and data security for computer systems is covered by a variety of federal laws and regulations, government bulletins, and other guiding documents.

EIV ACCESS, SECURITY, AND AVAILABILITY OF EIV DATA

The following reports will be printed as indicated:

- Existing Tenant Search/Move-In – As needed
    - If error occurs, the Owner/Agent will stop processing application until issue is resolved

- Multiple Subsidy Report – Monthly
    - When a multiple subsidy report error occurs, notify the tenant's last landlord to find out the correct move-out date and verify with the tenant. If the tenant has moved in and the move-in date overlaps the move-out date of the last landlord, you must terminate the tenant's lease (perform move-out) and charge the tenant market-rate rent for the number of days effected. Do an initial move-in with the correct dates.

- Identity Verification Report – Monthly
    - When an identity verification occurs, check the name and social security number against the tenant's birth certificate.

- Deceased Tenant's Report – Monthly
    - When a deceased tenant error occurs, ensure you update the systems to remove the deceased tenant from the records.

- New Hires Report – Requirements via HOTMA - Quarterly

OFFICE COPY

- Must be reviewed at least quarterly and stored as part of the Master File.
- The Owner/Agent reserves the right to review more frequently, as necessary.
- Will be reviewed when conducting Annual Recertifications (ARs)
- The Owner/Agent does not require families to undergo an Interim Recertification (IR) for earned income increases after submitting an IR to decrease earned income do not need to review this report between a family's ARs.
- The Owner/Agent requires an interim recertification (IR) for increases in earned income after submitting an IR to decrease earned income.
- The Owner/Agent will review the New Hires Report quarterly after submitting the IR to decrease earned income.

- Income Summary Report (Income Detail) - Requirements via HOTMA – Annually
  - Income Summary Reports will be reviewed at the annual recertification
  - Owner/Agents are no longer required to review this report when processing an interim recertification (IR).

- Income Report (Income Detail) - Requirements via HOTMA – Annually
  - Income Summary Reports will be reviewed at the annual recertification
  - Owner/Agents are no longer required to review this report when processing an interim recertification (IR).
  - Owner/Agents may use this report to verify any income shown in the report when paired with self-certification
  - Residents must indicate that the report is correct (or that they disagree with the data on the report) when using the report to verify specific information.
  - Owner/Agents are not required to use the report when processing the annual recertification if they used ***means-tested verification*** to determine the family's income for the current certification.
  - Income Detail Reports will be reviewed ***within 120 days*** of submission of the initial move-in transaction through TRACS.

- Income Discrepancy Report - Requirements via HOTMA
  - Upon the annual recertification, the Owner/Agent may discontinue using the EIV Income Discrepancy Report once the site software has been updated, and the residents have signed a renewal lease agreement.
    - NOTE: Because this report was designed to detect discrepancies related to a $200 income variance, it is no longer valid under HOTMA. This report will have to be revised by HUD before the data provided is meaningful (unless HUD eliminates the report entirely).
      - Once the report is modified, the Income Discrepancy Report must be reviewed at the annual recertification.
  - The Income Discrepancy Report is no longer required to be reviewed at any interim recertification under HOTMA
  - Owner/Agents are not required to use the report when processing an annual recertification if they used means-tested verification to determine the family's income for the current certification.

OFFICE COPY

- Owner/Agents are required to review the report ***within 120 days*** of submission of the move-in (MI / IC) transaction through TRACS.

SAFEGUARDING EIV DATA

The information processed by any EIV system can include wage and income data about private individuals, as well as identifying information such as Social Security Numbers, addresses, and employment information. This policy describes methods to comply with HUD's required safeguards.

Technical Safeguards

1. Reduce the risk of security violation related to the EIV system's software, network, or applications
2. Identify and authenticate all users seeking to use the EIV system data
3. Deter and detect attempts to access the system without authorization
4. Monitor the user activity on the EIV system

Administrative Safeguards

1. Ensure that access rights, roles, and responsibilities are appropriately and adequately assigned
2. Protect copies of sensitive data and destroy system-related records to prevent reconstruction of contents
3. Ensure authorized release of tenant information consent forms are included in all family files, before accessing and using data
4. Maintain, communicate, and enforce standard operating procedures relating to securing EIV data
5. Train staff on security measures and awareness, preventing the unauthorized accessibility of and use of data

Physical Safeguards

1. Establish barriers between unauthorized persons and documents or computer media containing private information
2. Clearly identify restricted areas by use of prominently posted signs or other indicators
3. Develop a list of authorized users who can access restricted areas (e.g. contractors, maintenance and janitorial personnel staff)
4. Prevent undetected entry into protected areas and/or documents
5. Notify Coordinators/Security Administrators of system breaches and penetration by unauthorized users

Designated Staff

1. Maintaining and enforcing the security procedures
2. Keeping records and monitoring security issues that may arise
3. Communicating security information and requirements to appropriate personnel including coordinating and conducting security awareness training sessions
4. Conducting review of all User IDs issued to determine if the users still have a valid need to access EIV data and taking necessary steps to ensure that access rights are revoked or modified as appropriate

OFFICE COPY

5. Reporting any evidence of unauthorized access or known security breaches to designated staff and taking immediate action to address the impact of the breach including but not limited to prompt notification to designated staff. Designated staff will escalate the incident by reporting to appropriate parties including the Contract Administrator or HUD

Limiting Access to EIV Data
User accounts for the EIV System will be provided on a need-to-know basis, with appropriate approval and authorization.

Security Awareness Training
Security Awareness Training is a crucial aspect

EIV System Coordinators
Before accessing EIV, the Executive Director will obtain a letter from the property manager/owner indicating that the owner gives permission for the EIV Coordinator to be responsible for UIV/EIV access and reports. Once permission is obtained, the EIV Coordinator will review the EIV training materials provided by HUD and complete the appropriate

EIV Users
Before requesting EIV User access, appropriate staff will review the EIV training materials provided by HUD and complete the appropriate Security Awareness Training Questionnaire and review the EIV Security Awareness Policy and the EIV User Policy. Upon completion of these three training courses, the EIV User will submit to the EIV Coordinator, the appropriate User Access Authorization Form. Upon receipt of the designated forms, the EIV Coordinator will recommend additional training, if necessary. If the EIV Coordinator feels that the EIV User candidate does not understand the security requirements, the EIV Coordinator will not continue with the EIV setup for that user.

Note: Under no circumstances will the EIV Coordinator process the User Access Authorization Form unless the executed Security Awareness Training Questionnaire, the signed EIV Security Policy and the signed EIV User Policy are attached.

Once the user request information is satisfactorily completed, the EIV Coordinator will complete the appropriate steps to provide EIV access to the user. In accordance with HUD requirements, the user's need for access will be reviewed on a quarterly basis.

At least once a year, staff with EIV access will be required to:

- Participate in training that includes a review of the EIV security policy and any HOTMA updates and
- Complete the EIV Security Awareness Training Questionnaire

The owner/agent will restrict access to EIV data only to persons whose duties or responsibilities require access to EIV. The EIV Coordinator will be required to request re-certification on an annual basis. EIV Coordinators are authorized to provide access only to those individuals directly involved in the resident certification process and/or compliance monitoring. EIV

OFFICE COPY

Coordinators will carefully review initial and quarterly requests for access and certify only those users who will need access within the next 90 days.

The owner/agent will ensure that a copy of the HUD Form 9887 and HUD Form 9887-A has been signed by each resident and members of the household 18 years of age or older. The 9887 will be presented at move-in and/or initial certification. If a household member turns 18 years of age in the middle of a certification cycle, that household member should sign the Form 9887 and Form 9887-A within seven days

The HUD 9887 Fact Sheet will be provided to all adult household members required to sign the form. By signing the forms, the applicant/resident authorizes HUD and/or the owner/agent to obtain and verify income and unemployment compensation information from various sources including, but not limited to the IRS, the Department of Health and Human Services, and the Social Security Administration, current and former employers and state agencies.

Resolving Discrepancies

The owner/agents are required to obtain written independent verification of disputed EIV data such as that provided by SSA and HHS' NDNH, in accordance with 24 CFR 5.236.

Following are the steps an owner/agent must take to resolve income discrepancies:

1. Notify and discuss any discrepancies with the resident
2. Request current documentation from the resident (i.e. originals, most recent (six months or more) consecutive pay stubs, original SSA benefits letter dated within the last 120 days, etc.) in accordance with Chapter 5, Paragraph 5-13 and 5-17, Determining Income and Calculating Rent, of Handbook 4350 3 REV-1, *Occupancy Requirements of Subsidized Multifamily Housing Programs*
3. Request written third-party verification of any income source that the tenant disputes
4. Confirm effective dates of unreported income
5. Provide the tenant with the right to contest the findings
6. Determine any retroactive rent due to the owner/agent in cases where the owner/agent confirms that the tenant failed to report income
7. Execute a repayment agreement with the tenant, when the tenant is unable to pay the amount due in full, in accordance with Chapter 8, Paragraph 8-20, A, Reimbursement to HUD for Overpayment of Assistance, of Handbook 4350.3 REV-1, *Occupancy Requirements of Subsidized Multifamily Housing Programs*
8. Adjust the rent, as necessary, in accordance with Chapter 7, Recertification's, Unit Transfers, and Gross Rent Changes of Handbook 4350.3 REV-1, *Occupancy Requirements of Subsidized Multifamily Housing Programs,* to reduce the occurrence of improper subsidy payments

Social Security Administration (SSA) Form 7004 form may be used by owner/agent to request a tenant's Social Security Earning Statement. The statement provides a record of the tenant's Social Security earnings history, year-by-year and provides an estimate of benefit payments that the tenant and the tenant's family may qualify for now or in the future.

OFFICE COPY

Owner/agents may not suspend, terminate, reduce or make a final denial of any financial assistance or payment under a federal benefit program against an individual, or take other adverse action against such individual, as a result of information produced by the EIV system without properly verifying the information and notifying the tenant in writing of any adverse findings in the same manner as applies to other information and findings relating to eligibility factors.

Owner/agents must reevaluate their policies and practices and review applicable regulations at 24 CFR 5.236 in light of availability of quarterly wage, unemployment compensation, and new hires employment information, and the possibility of a major increase in the number of cases of unreported and underreported tenant income.

Usernames, Password and Password Changes
Many systems require frequent changes in passwords. Secure Systems/EIV passwords will be changed in accordance with HUD Secure Systems requirements. Users will not share usernames or passwords with any other employee or with anyone outside of the organization. EIV access

Computer Systems Security Requirements
All computer systems and computers will have restricted access. The owner/agent will also use Antivirus software to limit data destruction or unintended transmission via virus, worms, Trojan horses or other malicious means. Remote access by other computers other than those specifically authorized is prohibited.

Authorized users of EIV data are directed to avoid leaving EIV data displayed on their computer screens where unauthorized users may view it. A computer will not be left unattended while the user is "logged" into Secure Systems. If an authorized user is viewing EIV data and an unauthorized user approaches the work area, the authorized user will lessen the chance of inadvertent disclosure of EIV data by minimizing or closing the screen on which the EIV data is being displayed.

Physical Security Requirements
The owner/agent may use a combination of methods to provide physical security for resident file records. The EIV data may be maintained in a locked metal file cabinet within a locked file room or office.

Restricted Areas
The owner/agent will have the areas clearly identified by the use of prominently posted signs or other indicators. For example, "Employees Only" signs. The sign should be posted on the door to the locked file room or office. The restricted areas will be separated from non-restricted areas by physical barriers that control access and/or will have limited access and points of entry.

Since the EIV data in resident files is maintained in the locked file room, designated staff will establish and maintain a key control log to track the inventory of keys available, the number of keys issued and to complete a form acknowledging the receipt of the key.

OFFICE COPY

Use and Handling of EIV Data
EIV data serves two purposes:

1. Verification of specific income information provided by the resident
2. Monitoring residents and staff compliance

Use of the data is described in the EIV User Policies. This policy is designed to provide protocol used to protect EIV data.

EIV Printouts
Reports available through EIV will not be printed to a shared printer unless the EIV user plans to immediately retrieve the data printed. It is preferred that all EIV printouts are sent to the user's personal printer. EIV printouts will be stored in the resident file in a separate folder/envelope. The documentation of EIV data will be included in the resident file. The entire file will be made available to authorized personnel including appropriate staff or contractors (i.e. Service Bureaus, contractors performing file reviews/audits, etc.) for the owner/agent, HUD staff, Contract Administration staff and the Office of Inspector General.

If other people are tasked with reviewing the file, such as financial auditors complying with the Consolidated Audit Guide (Handbook IG 2000.04), the EIV printout in the file/envelope including the EIV printout will be removed from the file and the Documentation of EIV Data will remain in the file to provide appropriate information required by the file audit.

If a resident requests a copy of their own EIV printout, a copy will be produced. The staff person providing the copy will note that the printout is a copy provided to the residents upon request. This note will include the following:

This is not an original, this a copy provided to the resident: _____ on this date: _____, 20__ by (Name of provider agent)
Initials: _____

The appropriate staff will make a note in the file any time a copy of the EIV data is obtained by authorized people and taken off site. This includes copies provided to the applicant/resident, other internal staff, HUD, CA, or OIG staff. Under no circumstances will the EIV information be provided to anyone other than that noted in this paragraph.

Other Language
Electronic information from EIV
Under no circumstances should anyone save or scan EIV information to retain an electronic copy. In order to ensure compliance with HUD's security requirements, EIV information should only be produced in a hard copy and maintained in accordance with the recordkeeping requirements outlined by HUD.

Alternative
In some cases, there may be a need to send or store EIV information electronically. If there is a need to store the information on a hard drive, a specific folder will be created. The folder will be

OFFICE COPY

password protected to prevent unauthorized access. Information in the folder will be purged periodically to comply with HUD's EIV file retention policies.

If EIV information is copied to portable media (i.e. CD, DVD, tape, etc.) that media will be destroyed appropriately upon completion of the intended use.

Reporting improper disclosure
Recognition, reporting, and disciplinary action in response to security violations are crucial to successfully maintaining the security and privacy of the EIV system. These security violations may include the disclosure of private data as well as attempts to access unauthorized data and sharing of User ID's and passwords. Upon the discovery of a possible improper disclosure of EIV information or other security violation by an employee or any other person, the individual making the observation or receiving the information will contact the EIV Coordinator and designated staff who will document all improper disclosures in writing providing details including who was involved, what was disclosed, how to disclosure occurred, and where/when it occurred. The EIV Coordinator will immediately review the report or improper disclosure and if appropriate, the EIV Coordinator will remove EIV access.

Improper disclosure of any information is grounds for immediate termination. All employees should carefully review the EIV Access Authorization Form to understand the penalties for improper disclosure of EIV data.

Disposal of EIV Information
EIV data will be destroyed in a timely manner based on the information provided in HUD's published EIV training materials, HUD notices or as prescribed by the owner/agent policy and procedures. The owner/agent's policy and procedures will not allow data retention that is longer than the time allowed in the published HUD materials.

As necessary, all EIV originals will be crosscut shredded or burned. Information about the use of EIV information and how printouts were destroyed will be maintained in the resident file.

This document will be given to all personnel maintaining, have access to Hobson City Apartments applicant and resident information. This document will also be made as part of the EIV Security Requirements, HOTMA updates, and the Tenant Selection Plan (TSP).

OFFICE COPY