KNOX COUNTY HOUSING AUTHORITY

Enterprise Income Verification (EIV) System
PHA Security Procedures

August 2012

Table of Contents

1.0 Introduction....1
1.1 Applicability....1
1.2 Purpose....1
1.3 Privacy Act Considerations....2
2.0 Safeguarding EIV Data....2
2.1 Limiting Access to EIV Data....3
2.1.1 Physical Security Requirements....3
2.1.2 Computer System Security Requirements....4
2.2 Disposal of EIV Information....5
3.0 Security Awareness Training....6
4.0 Record Keeping and Reporting Requirements....6
5.0 Reporting Improper Disclosures....6
6.0 PHA Security Assessment....8
Appendix 1. Safeguards Provided by the Privacy Act....13
Appendix 2. Criminal Penalties Associated with the Privacy Act....14
Appendix 3. Form HUD-9886, Authorization for the Release of Information/Privacy Act Notice....15
Appendix 4. PHA Access Authorization Form....17
Appendix 5. Key Accountability Record....18
Appendix 6. Acknowledgement of Receipt of Keys....19
Appendix 7. Restricted Area Access Register....20
Appendix 8. User Agreement....21
Appendix 9. Contractor Agreement....22
Appendix 10. EIV Disposal Log....23
Appendix 11. Security Awareness Training Attendance Record....24

1.0 Introduction

The Enterprise Income Verification System (EIV) is intended to provide a single source of income-related data to public housing agencies, including Knox County, for use in verifying the income reported by tenants in the various assisted housing programs administered by PHA's across the nation. The Office of Public and Indian Housing (PIH) is responsible for administering and maintaining the EIV system.

The EIV system assists the Knox County Housing Authority (KCHA) in the Enterprise verification of tenant income by comparing the tenant income data obtained from various sources including:

- Tenant-supplied income data captured on Form HUD-50058 and maintained in the Public Housing Information Center (PIC) databases;
- Wage information from the State Wage Information Collection Agencies (SWICAs);
- Social Security and Supplemental Security Income from the Social Security Administration; and,
- User Profile information from the PIC database.

EIV tenant data will only be used to verify a tenant's eligibility for participation in a HUD rental assistance program and to determine the level of assistance the tenant is entitled to receive. Any other use, **unless approved by the HUD Headquarters EIV Security System Administrator,** is specifically prohibited and may result in the imposition of civil or criminal penalties on the responsible person or persons. Further, no adverse action can be taken against a tenant until the PHA has independently verified the EIV information and the tenant has been granted an opportunity to contest any adverse findings through the established grievance, hearing, or other legal procedures.

1.1 Applicability

The Knox County Housing Authority will follow the procedures outlined in this document as they apply to all EIV data, regardless of the media on which they are recorded. Computerized media containing EIV data must be afforded the same levels of protection given to paper documents or any other media with EIV information.

1.2 Purpose

The purpose of this document is to provide guidance to assure that the practices, controls and safeguards used by the Knox County Housing Authority adequately protect the confidentiality of the tenant wage data and are in compliance with the Federal laws regarding the protection of this information. The Knox County Housing Authority will endeavor to integrate EIV documents and/or actions into its occupancy protocols, which also involve

Privacy Act related materials, e.g., third-party income, medical and other documents.

1.3 Privacy Act Considerations

The data provided via the EIV system must be protected to ensure that they are 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 are covered by a variety of Federal laws and regulations, government bulletins, and other guiding documents. The Privacy Act of 1974 as amended, 5 U.S.C. § 552 (a) is one such regulation and EIV data require careful handling in order to assure the Knox County Housing Authority compliance with the Privacy Act. (See *Appendix 1. Safeguards Provided by the Privacy Act.*) The Act also describes the criminal penalties associated with violation of policy supporting the Act. (See *Appendix 2. Criminal Penalties Associated with the Privacy Act.*)

The Knox County Housing Authority Security Officer, or designated staff, *must* assure that a copy of Form HUD-9886, Authorization for the Release of Information/Privacy Act Notice, has been signed by each member of the household age 18 years old or older and is in the household file. By signing this form, the tenant authorizes HUD and the PHA to obtain and verify income and unemployment compensation information from various sources including current and former employers, State agencies, and the SSA. HUD is relying on the Knox County Housing Authority to have this authorization on file as required by 24 CFR Part 5.230. Information obtained is protected under the Privacy Act. (See *Appendix 3. Form HUD-9886, Authorization for the Release of Information/Privacy Act Notice.)*

2.0 Safeguarding EIV Data

The information processed by the EIV system includes state wage and income data about private individuals, as well as identifying information such as Social Security Number, Address, and Employment information. As a condition of receiving the EIV data, the Knox County Housing Authority must establish and maintain certain safeguards designed to prevent unauthorized use of the information and to protect the confidentiality of that information.

The Knox County Housing Authority's Security Officer, or other designated staff, will have the responsibility of ensuring compliance with the PHA security policies and procedures outlined in this document. These responsibilities include:

- Maintaining and enforcing the security procedures;
- Keeping records and monitoring security issues;

- Communicating security information and requirements to appropriate personnel, including coordinating and conducting security awareness training sessions;
- Conducting a quarterly review of all User IDs issued to determine if the users still have a valid need to access the EIV data and taking the necessary steps to ensure that access rights are revoked or modified as appropriate; and
- Reporting any evidence of unauthorized access or known security breaches to the PHA Executive Director and taking immediate action to address the impact of the breach including but not limited to prompt notification to appropriate authorities including the HUD Field Office's Public Housing Director.

2.1 Limiting Access to EIV Data

The Knox County Housing Authority will restrict access to EIV data only to persons whose duties or responsibilities require access. The Knox County Housing Authority will maintain a record of users who have approved access to EIV data. Further, the KCHA will revoke the access rights of those users who no longer require such access or modify the access rights if a change in the user's duties or responsibilities indicates a change in the current level of privilege. (See Appendix 4. Enterprise Income Verification -the KCHA Access Authorization Form.)

EIV data will be handled in such a manner that it does not become misplaced or available to unauthorized personnel. Files containing EIV information will be color-coded or labeled clearly with the following statement "Confidential" or "For Official Use Only." To avoid inadvertent disclosures, the PHA staff may keep the EIV information separate from other information and files.

2.1.1 Physical Security Requirements

The KCHA may use a combination of methods to provide physical security for EIV data. These include, but are not limited to, locked containers of various types, locked rooms that have reinforced perimeters, and a locked building with guards. The EIV data may also be maintained in locked metal file cabinets within a locked room.

Access to the areas where EIV is maintained will be limited even during regular work hours. This may be accomplished by the use of restricted areas, a security room, or locked office space. By controlling the movement of individuals and eliminating unnecessary traffic through these critical areas, the PHA may reduce the opportunity for unauthorized disclosure of EIV data.

Restricted Areas: The KCHA will have any restricted areas clearly identified by the use of prominently posted signs or other indicators. For instance, a "For Authorized Personnel Only" or "Warning: Restricted Area" sign may be posted on the door or in the area. The restricted areas will be separated from non-restricted areas by physical barriers that control access and/or will have limited points of entry.

If the EIV data is maintained in a security room or locked space, the PHA Security Officer or designated staff will establish and maintain a key control log to track the inventory of keys available, the number of keys issued and to whom the keys are issued. All employees and contractors who have been issued keys to security rooms or locked spaces will complete a form acknowledging the receipt of the key. Combination locks will be changed or reset regularly, including whenever an employee leaves the PHA. (See *Appendix 5. Key Accountability Record* and *Appendix 6. Acknowledgement of Receipt of Keys.)*

The KCHA's Security Officer or designated staff will establish and maintain the list of users who can access the restricted area. The list will indicate the type of access that the user may have to the restricted area; it will indicate which users—such as contractors, maintenance, and janitorial/cleaning staff—must be escorted when entering the restricted area. The restricted area must be cleaned only during regular office hours or in the presence of an employee with authorized access. (See *Appendix 7. Restricted Area Access Register.*)

2.1.2 Computer System Security Requirements

The KCHA will avoid saving EIV data to a computer hard drive or any other automated information system. If EIV data is saved to a local machine at the HA office, the EIV data will be stored in a separate directory from other data maintained by the HA. Access to this directory will be restricted to authorized users of the EIV data. Diskettes may be used to record and store remarks or comments for the sole purpose of income verification. If used, the disk must be handled and secured in the same manner as the hard copy of the EIV data and must have a label which indicates "Confidential" or "For Official Use Only."

If EIV data is recorded on magnetic media with other data, it will be protected as if it were entirely EIV data. Such commingling of data sources on a single tape will be avoided, if practicable.

Users will retrieve computer printouts as soon as they are generated so that EIV data is not left lying unattended in printers where unauthorized users may access them. If possible, the HA will assign a dedicated printer for EIV use only in order to minimize the unauthorized interception of printed outputs from the EIV system.

Authorized users of EIV data will be directed to avoid leaving EIV data displayed on their computer screens where unauthorized users may view it. A computer will never be left

unattended with EIV data displayed on the screen. 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 out the screen on which the EIV data is being displayed.

User Accounts: User accounts for the EIV system will be provided on a need-to-know basis, with appropriate approval and authorization. The level of access granted determines the functionalities, features, and amounts of data within a specified PHA that the user can see. The KCHA Access Form will be used to request additions, deletions, or modifications of user accounts with access rights to the PIC system. (See Appendix 4. Enterprise Income Verification - PHA Access Authorization Form.)

All PHA employees and contractors who access the EIV system will have a current signed User Agreement on file. (See *Appendix 8. User Agreement* and *Appendix 9. Contractor Agreement*.) Users will maintain the security of their User Accounts by not disclosing their passwords to other staff members and not sharing user accounts with other employees or contractors. Users will not, deliberately or inadvertently, override the authorized access levels by providing EIV data to others who have limited or no access to the data. For instance, Mary has access to Reports A and B and Betty has access only to Report A. Mary will not provide Betty with printed copies of Report B. Nor will Mary allow Betty to access the system using her User Account as this would provide Betty with unauthorized access to Report B.

The March 2003 edition of the *PIC Help Newsbrief* provided a special coverage on security considerations for the KCHA. The article may be accessed at **http://www.hud.gov/offices/pih/systems/pic/newsletter/2003marnewsbrief.pdf.**

2.2 Disposal of EIV Information

EIV data will be destroyed as soon as it has served its purpose or as prescribed by the KCHA policy and procedures. All EIV originals and any documents created in association with their use will be either burned or shredded.

Burning precautions: The EIV material may be burned in an incinerator that produces enough heat to burn the entire bundle or the bundle will be separated to ensure that all pages are consumed.

Shredding precautions: To make reconstruction more difficult, the EIV documents may be inserted so that lines of print are perpendicular to the cutting line. Large amounts of shredded paper will not be allowed to accumulate in the bin.

It is important that a log or register be maintained of all documents that have been burned or shredded. (See *Appendix 10. EIV Disposal Log*)

3.0 Security Awareness Training

Security awareness training is a crucial aspect of ensuring the security of the EIV system and data. Users and potential users will be made aware of the importance of respecting the privacy of data, following established procedures to maintain privacy and security, and notifying management in the event of a security or privacy violation.

Before granting PHA employees and contractors access to EIV information, each employee and contractor must be trained in EIV security policies and procedures. Additionally, all employees having access to EIV data will be briefed at least annually on the security policy and procedures that require their awareness and compliance. The KCHA Security Officer or designated staff will record on a PHA form or record of Security Training all the users attending each briefing. (See *Appendix 11. Security Awareness Training Attendance Record*.)

On completion of security awareness training, the KCHA will make sure that employees or contractors who access the EIV data have completed a PHA User Agreement or PHA Contractor Agreement indicating that they are aware of the safeguards and responsibilities associated with using the system. (See *Appendix 8. User Agreement Form and Appendix 9. Contractor Agreement Form*.) Further, PHA employees will be advised of the penalties associated with the provisions of the Privacy Act of 1974, Section 552(a), which makes unauthorized disclosure or misuse of tenant wage data a crime punishable by a fine of up to $5,000. (See *Section 1.3 Privacy Act Considerations* and *Appendix 2. Criminal Penalties Associated with the Privacy Act.*)

The KCHA's Security Officer may communicate security information and requirements to appropriate personnel using a variety of methods outside of the formal training and awareness sessions. These methods may include:

- Discussions at group and managerial meetings; and
- Security bulletins posted throughout the work areas.

4.0 Record Keeping and Reporting Requirements

(This section is reserved for further development.)

5.0 Reporting Improper Disclosures

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 the sharing of User IDs and passwords. Upon the discovery of a possible improper disclosure of EIV information or another security violation by a PHA employee or any other person, the individual making the observation or receiving the information will contact the Its Security Officer and/or the Field Office's Office of Public Housing Director. The KCHA Security Officer or designated staff will document all improper disclosures in writing providing details including who was involved, what was disclosed, how the disclosure occurred, and where and when it occurred.

For additional information, contact the Chicago Field Office or HUD/PIH EIV Office.

6.0 PHA Security Assessment

Introduction

The practices and controls used by HUD and the KCHA to secure EIV information may be grouped into three categories: technical safeguards, administrative safeguards, and physical safeguards. Various technical safeguards have been built into the EIV systems to mitigate the risk of security violations. However, technical safeguards alone, without complementary physical safeguards and/or administrative safeguards do not meet HUD's standard for the protection of private data.

HUD has implemented various physical and administrative safeguards to complement the technical safeguards. The KCHA is strongly encouraged to take all reasonable steps to implement a combination of technical, physical, and administrative safeguards in order to assure that EIV data is appropriately secured. The physical and administrative safeguards that are implemented by a PHA must be appropriate when considered in combination with the technical safeguards available to the PHA through the EIV systems.

The security safeguards described throughout this *Security Guide* are consolidated below. The KCHA will assess their Privacy Act-related safeguards by reviewing the following safeguard options.

1. Technical Safeguards

A. Purposes of the Technical Safeguards

- Reduce the risk of a security violation related to the EIV systems' software, network, or applications
- Identify and authenticate all users seeking access to the EIV data
- Deter and detect attempts to access the system without authorization
- Monitor the user activity on the EIV systems

B. Description of the Technical Safeguards

The technical controls that have been built into the EIV systems address the following:

- User Identification and Authentication

- Each user is required to have their own User ID and Password
- The User ID identifies the PHA(s) and tenant information that the user is authorized to access
- Passwords are encrypted and the password file is protected from unauthorized access
- The system forces all users to change their password every 21 days and limits the reuse of previous passwords
- After three unsuccessful attempts to log in, the User ID is locked and the user has to contact the System Administrator to have the password reset

- Online User Alerts
  - Online warning messages that inform the user of the civil and criminal penalties associated with unauthorized use of the EIV data

2. Physical Safeguards

A PHA may implement any combination of the following physical safeguards that (a) meets acceptable standards for the protection provided by the specific safeguard, (b) accomplishes the purpose of the safeguards, and (c) conforms to standards of security stated here and elsewhere in this document.

A. Purposes of the physical safeguards

- Provide barriers between unauthorized persons and documents containing private data
- Provide barriers between unauthorized persons and computer media containing files that contain private data
- Prevent undetected entry to protected areas and/or to protected documents or computer media
- Provide immediate notification, noticeable under normal operating conditions, if the barrier is penetrated by unauthorized persons
- Prevent viewing or sensing of private information by any person by any means from outside the area confined by the barrier
- Allow authorized persons to have monitored and controlled access to protected private data

B. Alternatives for physical safeguards

- Locked and monitored buildings, offices, or storage rooms
- Locked and monitored metal file cabinets
- Designated secure areas and equipment
  - Security rooms or locked office space with limited (minimum required) points of entry (e.g., doors)
  - Security rooms or locked office space with limited (minimum required) means of entry (e.g., keys)
  - Restricted areas with prominently posted signs or other indicators identifying them and limited points of entry
  - Physical and administrative means for monitoring access to the secure areas and access and use of the protected data
  - Restricted use printers, copiers, facsimile machines, etc.
- Secure computer systems and output
  - Store EIV data in a separate, restricted-access directory if files are saved to local machine
  - Label all diskettes containing EIV data “Confidential” or “For Official Use Only”
  - Retrieve all computer printouts as soon as they are generated so that EIV data is not left lying unattended in printers
  - Avoid leaving a computer unattended with EIV data displayed on the screen
- Secure disposal of EIV information
  - Destroy as soon as it has served its purpose or as prescribed by the Its policy and procedures
  - All EIV originals and copies will either be burned or shredded

3. Administrative Safeguards

A PHA may implement any combination of the following administrative safeguards that (a) meets acceptable standards for the protection provided by the specific safeguard, (b) accomplishes the purpose of the safeguards, and (c) conforms to

standards of security stated here and elsewhere in this document.

A. Purposes of the administrative safeguards

- Ensure that access rights, roles, and responsibilities are appropriately and adequately assigned
- Maintain security-related records
- Monitor programmatic security issues
- Maintain, communicate, and enforce standard operating procedures related to securing EIV data
- Monitor access to protected private data located within the barriers of physical safeguards
- Control access to protected private data located within the barriers of physical safeguards

B. Alternatives for administrative safeguards

The KCHA will implement administrative safeguards to address the following:

- Assigning and Monitoring Access Rights
  - Determine which users will have access to EIV information
  - Maintain a record of all users who have approved access to EIV data including the date the access was granted and the date access was terminated
  - Ensure that all users who access the EIV system have a current signed *User Agreement* on file
  - Conduct a quarterly review of all User IDs to determine if the user still has a valid need to access the EIV data
  - Ensure that access rights are modified or revoked as appropriate

- Keeping Records and Monitoring Security Issues
  - Assure that a copy of *Form HUD-9886* has been signed by each adult member of the household and is kept in the household file
  - Maintain a key control log to track the inventory of keys available for secure buildings, rooms, or file cabinets, the number of keys issued and to whom the keys are issued

  - Ensure that all employees and contractors who have been issued keys to secure areas complete a form acknowledging the receipt of the key
  - Maintain a log of all users who access designated secure areas including the date and time of entry and exit and the purpose of the access
  - Ensure that combination locks are reset regularly, including whenever an employee leaves the PHA
  - Ensure that EIV information is disposed of in an appropriate manner
  - Maintain a log of all documents that have been burned or shredded including the name of the PHA employee who conducted the disposal, a description of the documents, the method of disposal, and the date of the disposal.

- Conducting Security Awareness Training
  - Ensure that all users of EIV data receive training in EIV security policies and procedures at the time of employment and at least annually afterwards
  - Maintain a record of all personnel who have attended training sessions
  - Communicate security information and requirements to appropriate personnel using various methods including discussions at group and managerial meetings and security bulletins posted throughout the work areas
  - Distribute all User Guides and Security Procedures to personnel using EIV data

- Reporting Improper Disclosures
  - Report any evidence of unauthorized access or known security breaches to the PHA Executive Director and the Chicago Field Office
  - Document all improper disclosures in writing
  - Report all security violations regardless of whether the security violation was intentional or unintentional

Appendix 1. Safeguards Provided by the Privacy Act

The Privacy Act provides safeguards for individuals against invasions of privacy by requiring Federal agencies, except as otherwise provided by law or regulation, to:

1. Permit individuals to know what records pertaining to them are collected, maintained, used, or disseminated;
2. Allow individuals to prevent records pertaining to them, obtained for a particular purpose, from being used or made available for another purpose without their consent;
3. Permit individuals to gain access to information pertaining to them, obtain a copy of all or any portions thereof, and correct or amend such records;
4. Collect, maintain, use, or disseminate personally identifiable information in a manner that ensures the information is current and accurate, and that adequate safeguards are provided to prevent misuse of such information;
5. Permit exemption from the requirements of the Act only where an important public policy need exists as determined by specific statutory authority; and
6. Be subject to a civil suit for any damages that occur as a result of action that violates any individual's rights under this Act.

Appendix 2. Criminal Penalties Associated with the Privacy Act

The Privacy Act of 1974 as amended, 5 U.S.C. § 552 (a)

(i)

1. CRIMINAL PENALTIES.--Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

2. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

3. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

Warnings in the EIV system welcome page provide a reminder each time the user logs in of the security considerations of the EIV system.

Appendix 3. Form HUD-9886, Authorization for the Release of Information/Privacy Act Notice

Authorization for the Release of Information/ Privacy Act Notice
to the U.S. Department of Housing and Urban Development (HUD) and the Housing Agency/Authority (HA)

U.S. Department of Housing and Urban Development
Office of Public and Indian Housing

PHA requesting release of information; (Cross out space if none) (Full address, name of contact person, and date)	IHA requesting release of information: (Cross out space if none) (Full address, name of contact person, and date)

Authority: Section 904 of the Stewart B. McKinney Homeless Assistance Amendments Act of 1988, as amended by Section 903 of the Housing and Community Development Act of 1992 and Section 3003 of the Omnibus Budget Reconciliation Act of 1993. This law is found at 42 U.S.C. 3544.

This law requires that you sign a consent form authorizing: (1) HUD and the Housing Agency/Authority (HA) to request verification of salary and wages from current or previous employers; (2) HUD and the HA to request wage and unemployment compensation claim information from the state agency responsible for keeping that information; (3) HUD to request certain tax return information from the U.S. Social Security Administration and the U.S. Internal Revenue Service. The law also requires independent verification of income information. Therefore, HUD or the HA may request information from financial institutions to verify your eligibility and level of benefits.

Purpose: In signing this consent form, you are authorizing HUD and the above-named HA to request income information from the sources listed on the form. HUD and the HA need this information to verify your household's income, in order to ensure that you are eligible for assisted housing benefits and that these benefits are set at the correct level. HUD and the HA may participate in computer matching programs with these sources in order to verify your eligibility and level of benefits.

Uses of Information to be Obtained: HUD is required to protect the income information it obtains in accordance with the Privacy Act of 1974, 5 U.S.C. 552a. HUD may disclose information (other than tax return information) for certain routine uses, such as to other government agencies for law enforcement purposes, to Federal agencies for employment suitability purposes and to HAs for the purpose of determining housing assistance. The HA is also required to protect the income information it obtains in accordance with any applicable State privacy law. HUD and HA employees may be subject to penalties for unauthorized disclosures or improper uses of the income information that is obtained based on the consent form. **Private owners may not request or receive information authorized by this form.**

Who Must Sign the Consent Form: Each member of your household who is 18 years of age or older must sign the consent form. Additional signatures must be obtained from new adult members joining the household or whenever members of the household become 18 years of age.

Persons who apply for or receive assistance under the following programs are required to sign this consent form:

- PHA-owned rental public housing
- Turnkey III Homeownership Opportunities
- Mutual Help Homeownership Opportunity
- Section 23 and 19(c) leased housing
- Section 23 Housing Assistance Payments
- HA-owned rental Indian housing
- Section 8 Rental Certificate
- Section 8 Rental Voucher
- Section 8 Moderate Rehabilitation

Failure to Sign Consent Form: Your failure to sign the consent form may result in the denial of eligibility or termination of assisted housing benefits, or both. Denial of eligibility or termination of benefits is subject to the HA's grievance procedures and Section 8 informal hearing procedures.

Sources of Information To Be Obtained

State Wage Information Collection Agencies. (This consent is limited to wages and unemployment compensation I have received during period(s) within the last 5 years when I have received assisted housing benefits.)

U.S. Social Security Administration (HUD only) (This consent is limited to the wage and self employment information and payments of retirement income as referenced at Section 6103(l)(7)(A) of the Internal Revenue Code.)

U.S. Internal Revenue Service (HUD only) (This consent is limited to unearned income [i.e., interest and dividends].)

Information may also be obtained directly from: (a) current and former employers concerning salary and wages and (b) financial institutions concerning unearned income (i.e., interest and dividends). I understand that income information obtained from these sources will be used to verify information that I provide in determining eligibility for assisted housing programs and the level of benefits. Therefore, this consent form only authorizes release directly from employers and financial institutions of information regarding any period(s) within the last 5 years when I have received assisted housing benefits.

Original is retained by the requesting organization. ref. Handbooks 7420.7, 7420.8, & 7465.1 form HUD-9886 (7/94)

Consent: I consent to allow HUD or the HA to request and obtain income information from the sources listed on this form for the purpose of verifying my eligibility and level of benefits under HUD's assisted housing programs. I understand that HAs that receive income information under this consent form cannot use it to deny, reduce or terminate assistance without first independently verifying what the amount was, whether I actually had access to the funds and when the funds were received. In addition, I must be given an opportunity to contest those determinations.

This consent form expires 15 months after signed.

Signatures:

Head of Household	Date		
Social Security Number (if any) of Head of Household		Other Family Member over age 18	Date
Spouse	Date	Other Family Member over age 18	Date
Other Family Member over age 18	Date	Other Family Member over age 18	Date
Other Family Member over age 18	Date	Other Family Member over age 18	Date

Privacy Act Notice. Authority: The Department of Housing and Urban Development (HUD) is authorized to collect this information by the U.S. Housing Act of 1937 (42 U.S.C. 1437 et. seq.), Title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d), and by the Fair Housing Act (42 U.S.C. 3601-19). The Housing and Community Development Act of 1987 (42 U.S.C. 3543) requires applicants and participants to submit the Social Security Number of each household member who is six years old or older. Purpose: Your income and other information are being collected by HUD to determine your eligibility, the appropriate bedroom size, and the amount your family will pay toward rent and utilities. Other Uses: HUD uses your family income and other information to assist in managing and monitoring HUD-assisted housing programs, to protect the Government's financial interest, and to verify the accuracy of the information you provide. This information may be released to appropriate Federal, State, and local agencies, when relevant, and to civil, criminal, or regulatory investigators and prosecutors. However, the information will not be otherwise disclosed or released outside of HUD, except as permitted or required by law. Penalty: You must provide all of the information requested by the HA, including all Social Security Numbers you, and all other household members age six years and older, have and use. Giving the Social Security Numbers of all household members six years of age and older is mandatory, and not providing the Social Security Numbers will affect your eligibility. Failure to provide any of the requested information may result in a delay or rejection of your eligibility approval.

Penalties for Misusing this Consent:

HUD, the HA and any owner (or any employee of HUD, the HA or the owner) may be subject to penalties for unauthorized disclosures or improper uses of information collected based on the consent form.

Use of the information collected based on the form HUD 9886 is restricted to the purposes cited on the form HUD 9886. Any person who knowingly or willfully requests, obtains or discloses any information under false pretenses concerning an applicant or participant may be subject to a misdemeanor and fined not more than $5,000.

Any applicant or participant affected by negligent disclosure of information may bring civil action for damages, and seek other relief, as may be appropriate, against the officer or employee of HUD, the HA or the owner responsible for the unauthorized disclosure or improper use.

Original is retained by the requesting organization. ref. Handbooks 7420.7, 7420.8, & 7465.1 form HUD-9886 (7/94)

Appendix 4. PHA Access Authorization Form

U.S. Department of Housing and Urban Development

Enterprise Income Verification – PHA Access Authorization Form

(Please Print or Type)

Housing Authority Name _____ PHA Code _____
(e.g. OH00X)

User Details

Type of Function (check one)

___ **New User in PIC** ___ Reset Password ___ Modify Access ___ Terminate User

___ **Existing PIC User** User's System ID (from HUD) _____

Social Security Number (SSN) _____ ____ _____

Authorized User's Name (Last, First & MI) Office Phone Number

_____ _____

Position Title _____

Office Address E-Mail Address

_____ _____
_____
_____

Type of Work which involves use of EIV information:_____
_____

Access Role: Voucher Occupancy _____ Public Housing Occupancy _____ Both _____

Limit to Following PH Development Numbers (Attached additional sheet if needed)_____
_____
_____

I authorize/request the above person access as indicated to the EIV System.

Executive Director's Name (Print)_____Date_____

Executive Director's Signature _____ Date_____

File in Security Control File

Appendix 5. Key Accountability Record

The Knox County Housing Authority

KEY ACCOUNTABILITY RECORD

KEY TO	TOTAL AVAILABLE	TOTAL ISSUED	PERSON ISSUED KEY

Last Update:

Appendix 6. Acknowledgement of Receipt of Keys

The Knox County Housing Authority

ACKNOWLEDGMENT OF RECEIPT OF KEYS

I _____ acknowledge receipt of
(Print Employee Name)

a key to the_____.
(State which File Cabinet or Door)

I understand that I:

1. Must not make unauthorized copies of key.
2. Must safeguard the key and not give it to anyone else.
3. Must not use the key to give access to unauthorized persons.

I also understand that unauthorized disclosure of Enterprise Income Verification (EIV) data can result in a felony conviction punishable by a fine of up to $5,000 and/or imprisonment up to five (5) years, as well as civil penalties. Also, unauthorized inspection of EIV can result in a misdemeanor penalty of up to $1,000 and/or one (1)-year imprisonment, as well as civil penalties.

_____ _____
Signature of Recipient Date

_____ _____
Signature of Security Manager/Officer Date

Appendix 7. Restricted Area Access Register

The Knox County Housing Authority Restricted Area Access Register

Full Name (Last, First, MI)	Signature	PHA Employee	Entry		Departure	
			Date	Time	Date	Time

Appendix 8. User Agreement

USER AGREEMENT

The Knox County Housing Authority

As an authorized user of Enterprise Income Verification (EIV) information, I understand the information obtained may only be used for official PHA business.

I understand my user ID and password is to be used only by me. Under no circumstances will I reveal or allow use of my password by another person.

I understand any printed EIV data must be stored in a locked container or room and it must be shredded, burned or otherwise destroyed when no longer needed.

I understand if I fail to follow any of the Its or HUD's standards, I may be subject to disciplinary action and/or prosecution. Willful unauthorized disclosure of EIV can result in a felony conviction punishable by a fine up to $5,000 and/or imprisonment up to five (5) years, as well as civil penalties. Also, willful unauthorized inspection of EIV can result in a misdemeanor penalty of up to $1,000 and/or one (1)-year imprisonment, as well as civil damages.

I understand and agree to follow the security procedures stated in this agreement.

_____	_____	_____
Employee Signature	Printed Employee Name	Date

Appendix 9. Contractor Agreement

CONTRACTOR ACKNOWLEDGMENT

The Knox County Housing Authority

As a contractor assigned to work on-site in the PHA, I understand that only authorized PHA employees may access, disclose, inspect and use Enterprise Income Verification (EIV) data.

I also understand that the penalty for unauthorized disclosure or inspection of EIV by a federal employee also applies to contractors. Also, I understand that willful unauthorized inspection of EIV can result in civil and criminal penalties. The penalties are as follows:

- **Unauthorized disclosure** can result in a felony conviction and a fine up to $5,000 and/or imprisonment up to five (5) years, as well as civil penalties.

- **Unauthorized inspection** of EIV can result in a misdemeanor penalty of up to $1,000 and/or one (1)-year imprisonment, as well as civil damages.

I understand that my user ID and password is to be used only by me. Under no circumstances will I reveal or allow use of my password by another person. Nor will I use another person's password and user ID.

I understand and agree to follow all PHA standards, policies and procedures.

_____	_____	_____
Contractor Signature	Printed Contractor Name	Date

Appendix 10. EIV Disposal Log

The Knox County Housing Authority

EIV Disposal Log

Name of PHA Employee	What was Disposed	How	Date

Appendix 11. Security Awareness Training Attendance Record

The Knox County Housing Authority

Security Awareness Training

Attendance Record

Instructor: _____ **Date of Training:** _____

Employee/ Contractor Name	*Employee/ Contractor Signature*	*Business Area/Office*
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		