U.S. Department of Housing and Urban Development

Enterprise Income Verification System (EIV)

Security Procedures for Upfront Income Verification (UIV) data

---

Version 1.4, November 2005

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 3
2.1 Limiting Access to EIV Data 3
2.1.1 Physical Security Requirements 4
2.1.2 Computer System Security Requirements 5
2.2 Destruction of Records and Clearing of Various Types of Automated Media 6
3.0 Security Awareness Training 8
4.0 Record Keeping and Reporting Requirements 9
5.0 Reporting Improper Disclosures 12
6.0 Program Administrator Security Assessment 13
Appendix 1. Safeguards Provided by the Privacy Act 18
Appendix 2. Criminal Penalties Associated with the Privacy Act 19
Appendix 3. Form HUD-9886, Authorization for the Release of Information/Privacy Act Notice 20
Appendix 4. Access Authorization Form for Program Administrators 22
Appendix 5. HUD/PHA Access Authorization Form 26
Appendix 6. Key Accountability Record 28
Appendix 7. Acknowledgement of Receipt of Keys 29
Appendix 8. Restricted Area Access Register 30
Appendix 9. Guide for Cleaning or Sanitizing Media 31
Appendix 10A. Media Destruction Log 33
Appendix 10B. EIV Disposal Log 34
Appendix 11. Security Awareness Training Attendance Record 35
Appendix 12. Reference Listing 36

1.0 Introduction

The Enterprise Income Verification System (EIV) is a system intended to provide a single source of income-related data to PHAs and HUD (hereafter referred to as program administrators) for use in verifying the income reported by tenants participating in the various assisted housing programs. The Office of Public and Indian Housing (PIH) is responsible for administering and maintaining the EIV system. The EIV system assists the program administrators in the upfront verification of tenant income by comparing the tenant income data obtained from various sources including:

- Tenant-supplied income data is captured on Form HUD-50058 – Family Report and maintained in the Public Housing Information Center (PIC) database;
- Department of Health and Human Services' National Directory of New Hires Data (NDNH)
- Social Security and Supplemental Security Income from the Social Security Administration; and,
- User Profile information from the PIC database.

Upfront income verification (UIV) tenant data should 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 Coordinator or EIV Security Officer,** 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 program administrator has independently verified the UIV 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 procedures outlined in this document apply to program administrators that have access to the EIV system and UIV data and administering the: Public Housing and the Housing Choice Voucher Programs. The procedures outlined in this document apply to all UIV data, regardless of the media on which they are recorded. Computerized media containing UIV data must be afforded the same levels of protection given to paper documents or any other media with UIV data.

1.2 Purpose

The purpose of this document is to provide guidance to assure that the practices, controls and safeguards used by program administrators adequately protect the confidentiality of the tenant wage data and are in compliance with the Federal laws regarding the protection of this information. Program administrators should integrate UIV documents and/or actions into

the PHA's 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 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 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 program administrators' 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.*)

HUD has interagency agreements with:

- the Social Security Administration for the social security (ss) and the supplemental security income (ssi) data and
- the HHS's Office of Child Support Enforcement for information furnished from the National Directory of New Hires (NDNH) data.

Under the Privacy Act, tenants have the right to challenge the accuracy of information maintained by the Federal government that concerns them. If a tenant disputes the employment and/or income information, the tenant must contact the employer. If the information is incorrect, the employer must correct the information and resubmit it to the state, IRS and HHS. The employer is the originator of the data.

If the tenant disputes the SS/SSI information, the tenant must contact SSA. If the SS/SSI information is incorrect, SSA must correct the information and update its database. SSA is the originator of the data.

The program administrator's Security Officer, or designated staff, *must* assure that a copy of Form HUD-9886 - Authorization for the Release of Information/Privacy Act Notice, or an equivalent consent form that meets the requirements under 24 CFR 5.230**,** 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 program administrator to obtain and verify income and unemployment compensation information from various sources including current and former employers, State agencies, SSA and HHS. HUD is relying on program administrators to have this authorization form 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 but may not be limited to income data about private individuals; it may identify such information as Social Security Number, Address, and employment information. Once information from the EIV system becomes a part of a system maintained by the program administrator, that system and the information it contains becomes the responsibility of the program administrator. This section focuses on the procedures to be followed when UIV data becomes part of the program administrator's case files as part of the recertification process.

As a condition of receiving the UIV data, program administrators must establish and maintain certain safeguards designed to prevent unauthorized use of the information and to protect the confidentiality of that information. .

The program administrator's Security Officer, or other designated staff, will have the responsibility of ensuring compliance with the program administrator's 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 staff, 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 (See Section 5.0 – Reporting Improper Disclosures

2.1 Limiting Access to EIV Data

The program administrators should restrict access to UIV data only to persons whose duties or responsibilities require access. Appendix 5 provides a copy of the EIV Access Authorization Form. The program administrators should maintain a record of users who have approved access to UIV data. Further, the program administrators should 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 Section 2.1.2 – User Accounts. Ensure that users sign the EIV

Rules of Behavior and User Agreement form (Appendix 4) which provides general instructions on the appropriate use of the EIV resources and apply to all EIV users, including all program administrators and contractors.

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

2.1.1 Physical Security Requirements

Program administrators may use a combination of methods to provide physical security for UIV 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 UIV data may also be maintained in locked metal file cabinets within a locked room.

Access to the areas where UIV data is maintained should 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, program administrators may reduce the opportunity for unauthorized disclosure of UIV data.

Restricted Areas: Program administrators should 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 should be separated from non-restricted areas by physical barriers that control access and/or should have limited points of entry.

If the UIV data is maintained in a security room or locked space, the program administrator, security officer or designated staff should 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 should complete a form acknowledging the receipt of the key. Combination locks should be changed or reset regularly, including whenever an employee leaves the program administrator's staff or office (See *Appendix 6. Key Accountability Record* and *Appendix 7. Acknowledgement of Receipt of Keys.)*

The program administrator security officer or designated staff should establish and maintain the list of users who can access the restricted area. The list should indicate the type of access that the user may have to the restricted area; it should 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 8. Restricted Area Access Register.*)

2.1.2 Computer System Security Requirements

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

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

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

Authorized users of UIV data should be directed to avoid leaving UIV data displayed on their computer screens where unauthorized users may view it. A computer should never be left unattended with UIV data displayed on the screen. If an authorized user is viewing UIV data and an unauthorized user approaches the work area, the authorized user should lessen the chance of inadvertent disclosure of UIV data by minimizing or closing out the screen on which the UIV data is being displayed.

User Accounts: User accounts for the EIV system should 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 program administrator jurisdiction or area of authority that the user can see. The EIV Access Authorization Form should be used to request additions, deletions, or modifications of user accounts with access rights to the WASS system. The EIV User and Operations manuals (http://hudstage.hud.gov/offices/pih/programs/ph/rhiip/uivsystem.cfm) provide instructions on the use of the EIV system. It also focuses on the end user functionality and administration used for viewing tenant income.

All program administrator employees and contractors who access the EIV system should have a current signed Rules of Behavior and User Agreement on file. Users should 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 should not, deliberately or inadvertently, override the authorized access levels by providing UIV data to others who have limited or no access to the data. For instance, Mary has access to Projects A and B and Betty has access only to Project A. Mary should not provide Betty with printed copies of Report B. Nor should Mary allow Betty to access the system using her User Account to have access as this would provide Betty with unauthorized access to Project B.

2.2 Destruction of Records and Clearing of Various Types of Automated Media

EIV data should be destroyed as soon as it has served its purpose or as prescribed by the program administrators's policy and procedures. (See Appendix 9 and 10) All UIV originals and any documents created in association with their use can be either shredded or burned to prevent the reconstruction of the contents.

It is essential that the methods used to dispose of records are thorough. This applies to both the destruction of record copies pursuant to records schedules as well as copies of records that are no longer needed (See HUD Handbook Nos. 2225.6 REV-1, CHG-49, 2228.1 and 2229.1 for HUD Records Disposition Schedules and Scheduling for Automated Systems.)

If shredding is the process used for disposition: paper should be shredded to effect 5/16 inch wide or smaller strips and microfilm should be shredded to effect 1/35-inch by 3/8 – inch strips. The industry standard is currently ½", however the strips can be larger than 5/16"; the strips must be unreadable. Large amounts of shredded paper should not be allowed to accumulate in the bin.

Magnetic tape containing UIV data must not be made available for reuse by other offices or released for destruction without first being subjected to repeated electromagnetic erasing (not less than three complete passes). It should also be noted what type of machine was used for the electromagnetic erasing. If reuse of the tapes is not intended, the tapes should be destroyed by cutting into lengths of 18 inches or less or by burning them to get a complete incineration.

If disk media is used, any UIV data on it must be destroyed by completely overwriting all data tracks a minimum of three times, using maximum current that will not damage or impair the recording equipment or by running a magnetic strip of sufficient length to reach all areas of the disk over and under each surface a minimum of three times. If the information on the disk cannot be destroyed, the disk should be damaged in a manner that would prevent its use in any disk drive unit and then discarded.

Optical disks that are not re-writable such as CDs and DVDs must be shredded in a manner similar to paper shredding. A media disposal checklist should be used to indicate if the media was destroyed, to be used for surplus

or reuse. **Hand tearing, recycling or burying information in a landfill is an unacceptable method of disposal of UIV data.**

If the agency uses a contractor for the shredding or other record destruction process, it is recommended that the contractor certify to the destruction. If shredding is not to take place on site in the presence of an agency employee, then it is important that the terms of the contract notify the contractor of their responsibility to protect sensitive information and potential liability for unauthorized use or disclosure of personal information. Contractor personnel are to certify that they have knowledge or have receive training in security procedures (regarding Privacy Act data) used to protect documents prior to their destruction.

(See Appendix 9 for suggested methods of cleaning or sanitizing various types of media and sample media disposal checklist. This information was obtained from the Department of Health and Human Services Information Security Program Handbook [11-12-04], Appendices I and J).

Burning precautions: If burning is the process for disposition of the UIV material, it may be burned in an incinerator that produces enough heat to burn the entire bundle or the bundle should be separated to ensure that all pages are consumed.

It is important that a log or register be maintained of all documents and media that have been burned, shredded or destroyed. (See Appendix 10A and 10B for samples of EIV disposal/destruction logs.)

3.0 Security Awareness Training

Security awareness training is a crucial aspect of ensuring the security of the EIV system and UIV data. Users and potential users should 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 employees and contractors access to UIV information, each employee and contractor must be trained in EIV security policies and procedures. Additionally, all employees having access to UIV data should be briefed at least annually on the program administrator's security policy and procedures that require their awareness and compliance. The program administrator security officer or designated staff should record on a program administrator 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 program administrators should make sure that employees or contractors who access the UIV data have completed a Rules of Behavior and User Agreement indicating that they are aware of the safeguards and responsibilities associated with using the EIV system. Further, program administrator employees should 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 program administrator 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

The records that are maintained by program administrators in implementing the EIV system are to be consistent with HUD records schedules that have been created to meet legal requirements for records management as administered by the National Archives and Records Service pursuant to 42 U.S.C. 21. The records are to be maintained for at least five years or as prescribed by the applicable program administrator's records control policy or procedures, whichever is longer. In addition, UIV records (both electronic and paper) and the information contained in them must be used only for their intended purpose (the administration of Federal rental assistance programs and determining tenant income eligibility) to avoid unintentional disclosures of personal private information, which would be a violation the Privacy Act of 1974.

The agreement with the Social Security Administration (SSA) to provide the social security and supplemental security information data and the HHS's Office of Child Support Enforcement to provide the income data from the National Directory of New Hires (NDNH) specifies that **any incorrect information or challenge to the accuracy of information that these agencies furnish is to be referred to the agencies for disposition and not the program administrators.**

Once information from UIV information becomes part of a system maintained by the program administrator, that system and the information that it contains becomes the responsibility of the program administrator. This document focuses on the policies and procedures to be followed when UIV information becomes part of program administrator's case files as part of the recertification process or the review thereof.

Record Keeping Requirements

The EIV system presently does not support downloading of information by users. At such time as it does, it will be the responsibility of the program administrator to securely maintain that information from unauthorized access and unwarranted disclosure. Reports and screen prints of UIV information are to be maintained securely. (See Section 6 – Program Administrator Security Assessment, subsection 3 – Administrative Safeguards.

Protection of copies of records and the information within them

Xerox copies, spreadsheets, files or records that contain personal information derived from the UIV data are to be protected from unauthorized access and inadvertent disclosure. These documents are to be destroyed in accordance with the information in Section 2.2 – Disposal of EIV Information.

UIV screens that contain personal information and reports are also covered by the Privacy Act. Labeling documents as private is a protection against

inadvertent disclosure. All documents, file folders/cabinets or electronic storage media created by program administrators containing personal information from UIV or derived using UIV data are to be labeled "Confidential." An exception from the labeling requirement is for documents derived from UIV data that are purely summary in nature, such as data aggregated at the program administrator level. The files, when not in use, are to be locked away from physical access and are to be password protected if they are on a computer.

Official file copies of Public Housing program records, UIV user administration and UIV security administration records are only to be disposed of not sooner than within 5 years of creation and following the approved program administration schedule.

Access to UIV information.

UIV information is available to program administrator staff within the scope of their responsibilities for the administration of Public Housing and Housing Choice Voucher Programs and for the administration of the EIV system itself. Thus, program administrator staff may only access records within the scope of their duties, which typically concern only their own PHA and program area. The scope of individual responsibilities may be assigned within the scope of specific Public Housing developments or projects.

Some program administrators administer rental assistance programs for other program administrators under a contract(s) or cooperative agreement(s) and individual assignments covering more than one PHA are to be documented in the application for access in the User Administration file.

When a program administrator services more than one PHA, project and/or contract, the records from the different program administrators are not to be co-mingled with other program administrators file records and/or data.

The scope of responsibility of anyone who accesses the EIV system is documented in the EIV User Administration file and the User Administrator or Security Administrator/Officer should be consulted if there is an issue. The Security Administrator/Officer also is to be consulted if there is an issue regarding access by individuals who do not have access to EIV system but who may be responsible for occupancy specialist type functions.

Any issue regarding the possible disclosure to third parties of information from UIV files, including records derived from those files and case files in which UIV data has been incorporated should be referred to the program administrator security officer or designee responsible (in writing). If a security violation may already have occurred such as improper disclosure of information to a third party, the program administrator's security officer or designee should notify program administrator's security administrator and/or the HUD Office of Inspector General. See Section 5.0 – Reporting Improper Disclosures.

Program administrator staff should not re-disclose the UIV data it receives without proper authorization from the program administrator's security officer or designee. When the re-disclosure of the UIV data is authorized,

information disclosed outside of the program administrator's office/agency must be recorded on a list, which reflects to whom the disclosure was made, what was disclosed, why and when it was disclosed and when and if it was returned.

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 UIV information or another security violation by a program administrator employee or any other person, the individual making the observation or receiving the information should contact the program administrator's security officer and/or the Field Office's Office of Public Housing Director. The program administrator security officer or designated staff should 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.

The following contacts should be made:

- The program administrator security officer should contact and provide the PHA Executive Director or the designee with the written documentation;
- The PHA Executive Director or the designee should provide the HUD Field Office Public Housing Director with the written documentation; and,
- The HUD Field Office Public Housing Director upon receipt of the written documentation will make a determination regarding the referral and the provision of the written documentation to the Headquarters EIV Coordinator and/or EIV Security Officer for further review and follow-up action.

6.0 Program Administrator Security Assessment

Introduction

The practices and controls used by HUD and program administrators to secure upfront income verification information may be grouped into three categories: technical safeguards, administrative safeguards, and physical safeguards. Various technical safeguards have been built into the EIV system 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. Program administrators are 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 program administrator must be appropriate when considered in combination with the technical safeguards available to the program administrator through the EIV system.

The security safeguards described throughout this *Security Guide* are consolidated below. Program administrators should 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 system's software, network, or applications
- Identify and authenticate all users seeking access to the UIV data
- Deter and detect attempts to access the system without authorization
- Monitor the user activity on the EIV system

B. Description of the Technical Safeguards

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

- User Identification and Authentication
  - Each user is required to have their own User ID and Password
  - The User ID identifies the program administrators 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 UIV data

2. Physical Safeguards

A program administrator 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 UIV data in a separate, restricted-access directory if files are saved to local machine
  - Label all diskettes containing UIV data "Confidential" or "For Official Use Only"
  - Retrieve all computer printouts as soon as they are generated so that UIV data is not left lying unattended in printers
  - Avoid leaving a computer unattended with UIV data displayed on the screen

- Secure disposal of UIV information
  - Destroy as soon as it has served its purpose or as prescribed by the PHA's policy and procedures
  - All UIV originals and copies should either be burned or shredded

3. Administrative Safeguards

A program administrator 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 UIV 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

Program administrators should implement administrative safeguards to address the following:

- Assigning and Monitoring Access Rights
  - Determine which users should have access to UIV information
  - Maintain a record of all users who have approved access to UIV 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 UIV data
  - Ensure that access rights are modified or revoked as appropriate

- Keeping Records and Monitoring Security Issues
  - Assure that a copy of *Forms HUD-9886* or HUD 9887 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 program administrator's staff or office
  - Ensure that UIV 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 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 UIV data receive training in UIV 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 UIV data

- Reporting Improper Disclosures
  - Report any evidence of unauthorized access or known security breaches to the PHA Executive Director and the HUD Field Office Public Housing Director)
  - 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. Access Authorization Form for Program Administrators

Enterprise Income Verification (EIV) System

Rules of Behavior and User Agreement

HUD Office or Field Office Name: _____ **HUD Field Office Code**: _____

(To be completed by HUD employees/contractors) (e.g. 1HBOS)

PHA Name: _____ **PHA Code**: _____

(To be completed by PHA employees/contractors) (e.g. MD999)

A. Rules of Behavior

1. Introduction

The U.S. Department of Housing and Urban Development (HUD), Public and Indian Housing Real Estate Assessment Center (PIH-REAC) is actively involved in implementing and maintaining Office Departmental policies and procedures to keep PIH-REAC Systems secure from unauthorized access and inappropriate use. In compliance with various security-related Federal laws and regulations, PIH-REAC created these of rules of behavior for the Enterprise Income Verification (EIV) system. This document was created to ensure that EIV system users comply with HUD and PIH-REAC security policies. In addition, this document ensures that system accounts remain secure and are used in the appropriate manner.

PIH-REAC may grant limited system access to users (e.g. HUD employees, contractors, clients/customers, and program participants) who have a need to utilize the PIH-REAC information resources. EIV resources are for official use only. As a condition of receiving access, you are required to understand and abide by the HUD and PIH-REAC's EIV system security policies and procedures. The purpose of these policies and procedures is to safeguard the PIH-REAC's valuable information resources.

All EIV users must adhere to the Rules of Behavior outlined in this document. 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. This may include removal of system access for a specific period of time or termination depending on the severity of the violation. See Section B for potential civil and criminal penalties.

2. Responsibilities

The System Owner is responsible for ensuring that an adequate level of protection is afforded to the EIV system through an appropriate implementation of technical, operational, and managerial security controls.

EIV system users are responsible for the protection of passwords, information, equipment, systems, networks, and communication pathways to which they have access. All HUD computer resources including hardware, software, programs, files, paper reports, and data are the sole property of HUD.

3. Other Policies and Procedures

The Rules of Behavior do not replace existing HUD or PIH-REAC policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing the EIV system. The rules are consistent with the policy and procedures described in the following security documents:

HUD Security Program Policy The policy, HUD Handbook 2400.25, Rev. 1 dated May 2005, prescribes responsibilities, practices, and conditions that directly or indirectly promote security in the development, operation, maintenance, and support of all HUD IT resources.

4. Application Rules

The Web Access Security System (WASS) user identification (userID) and password issued to you are to be used solely in connection with the performance of your responsibilities in support of HUD's mission and may not be used for personal or private gain. You agree to be responsible for the confidentiality of the assigned information and accountable for all activity with your userID. Furthermore, you agree that you will not provide this confidential userID/password to another user during employment and upon leaving the employment of the Department. Additional rules of the EIV system are as follows:

System Access (on-site only) – Users are required to use only approved HUD software, software settings, and comply with vendor software license agreements. Users are allowed to access the system only using the mechanisms specified by PIH-REAC.

Unofficial use of government information – Users must be aware that personal use of information resources is prohibited. EIV data is personal information covered by the Privacy Act and penalties apply to the misuse of that data.

Information protection – Users must avoid leaving system output records or reports unattended or unsecured. Users should lock the computer or log-out of the system when leaving work areas unattended. Users shall not violate Public Law 93-579, Privacy Act of 1974, which requires confidentiality of personal data contained in government and contractor data files. Users should back up their data, test the data backups, and securely store the data in accordance with PIH-REAC policy.

Use of passwords – User passwords and userIDs are for your individual use only and are confidential HUD information. Users are required to change passwords every 21 days. Users are encouraged to avoid creating passwords that can be easily associated with.

System privileges – Users are given access to the system based on a need to perform specific work. Users shall only access the information for which they are authorized.

Individual accountability – Users shall be held accountable for their actions while accessing the system. Be aware that all computer resources are monitored and audited.

Incident Response – Users should contact their supervisor and the PIH-REAC Security Officer immediately regarding any suspected violation or breach of system security.

B. User Agreement

I have read the above policy regarding system security awareness and practices when accessing PIH-REAC's information technology resources. I understand the policies and procedures as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Enterprise Income Verification System and data.

As an authorized user of the Enterprise Income Verification System, I understand the information obtained may only be used for official HUD/PHA business. I understand that only authorized HUD or PHA employees may access, disclose, inspect and use upfront income verification (UIV) data.

I also understand that willful unauthorized inspection of UIV data can result in civil and criminal penalties. The penalties are as follows:

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

- **Unauthorized inspection** of UIV data 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 are 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 HUD/PHA standards, policies and procedures.

_____	_____	_____
EIV System User's Name (Signature)	EIV System User's Name (Print)	Date

Copy – File

Appendix 5. HUD/PHA Access Authorization Form

Enterprise Income Verification (EIV) System
HUD/PHA Access Authorization Form

(Please Print or Type)

Date of Request: _____

HUD Office Name: _____ HUD Field Office Code: _____
(To be completed by HUD users) (e.g., 1HBOS)

PHA Name: _____ PHA Code: _____
(To be completed by PHA users) (e.g., MD999)

Type of Function Required (check one)

☐ Add Access ☐ Terminate User ☐ Modify Access _____
(Provide details of modification request)

Authorized User Details

Name: (Last, First, and Middle Initial) _____ WASS User ID: _____

Position Title: _____ Phone Number: _____

Email Address: _____ Fax Number: _____

Type of work which involves use of UIV data: _____

_____

Check all that apply

Access Level: ☐ HUD Headquarters ☐ HUB ☐ Field Office ☐ TARC ☐ PHA

PHA User Access Role: ☐ PHA Occupancy – Public Housing ☐ PHA Occupancy – Voucher ☐ PHA User Administrator ☐ PHA Security Administrator

HUD User Access Role: ☐ Occupancy Specialist ☐ User Administrator ☐ Security Administrator

Specify the Project Numbers and/or PHA Codes to which access will be limited. Continue the list on a separate sheet, if necessary, or put "All".

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

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

	Name (Print)	Signature	Date
HUD Headquarters UIV Coordinator:			
Public Housing Director: (Field Office users only)			
Executive Director or Designee: (PHA users only)			

Copy 1 – File

Appendix 6. Key Accountability Record

Program Administrator Name_____

KEY ACCOUNTABILITY RECORD

KEY TO	TOTAL AVAILABLE	TOTAL ISSUED	PERSON ISSUED KEY

Last Update:

Appendix 7. Acknowledgement of Receipt of Keys

Program Administrator

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 data 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 8. Restricted Area Access Register

Program Administrator Restricted Area Access Register

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

Appendix 9. Guide for Cleaning or Sanitizing Media

Methods of Cleaning or Sanitizing Various Types of Media

Media	Clear	Sanitize
Magnetic Tape		
Degaussing Type I	a or b	a, b, or m
Degaussing Type II	a or b	b or m
Degaussing Type III	a or b	m
Magnetic Disk		
Bernoullis	a, b, or c	m
Floppies	a, b, or c	m
Nonremovable Rigid Disk	c	a, b, d, or m
Removable Rigid Disk	a, b, or c	a, b, d, or m
Optical Disk		
Read Many, Write Many	c	m
Read Only		m, n
Write Once, Read Many (WORM)		m, n
Memory		
Dynamic Random Access Memory (DRAM)	c or g	c, g, or m
Electronically Alterable PROM (EAPROM)	i	j or m
Electronically Erasable PROM (EEPROM)	i	h or m
Erasable Programmable ROM (EPROM)	k	l, then c, or m
Flash EPROM (FEPROM)	i	c then i, or m
Programmable ROM (PROM)	c	m
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	m
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m
Read-Only Memory (ROM)		m
Static Random Access Memory (SRAM)	c or g	c and f, g, or m
Equipment		
Cathode Ray Tube (CRT)	g	q
Printers		
Impact	g	p then g
Laser	g	o then g

Table Key

(a) Degauss with a Type I degausser. Type I degaussers are equipment rated to degauss magnetic media having a maximum coercivity of 350 Oersteds.
(b) Degauss with a Type II degausser. Type II degaussers are equipment rated to degauss magnetic media having a maximum coercivity of 750 Oersteds.
(c) Overwrite all addressable locations with a single character.
(d) Overwrite all addressable locations with a character, its complement, and then a random character. Verify. This method is NOT approved for sanitizing media containing Top Secret information.
(e) Overwrite all addressable locations with a character, its complement, and then a random character.
(f) Each overwrite must reside in memory for a period longer than the period during which the classified data resided.
(g) Remove all power including battery power.
(h) Overwrite all locations with a random pattern, all locations with binary zeros, and all locations with binary ones.
(i) Perform a full chip erase as directed by the manufacturer's data sheets.
(j) Perform (i) above, then (c) above, for a total of three times.
(k) Perform an ultraviolet erase as directed by the manufacturer's data sheets.
(l) Perform (k) above, but increase the time by a factor of three.
(m) Destroy—disintegrate, incinerate, pulverize, shred, or melt.
(n) Perform the required destruction only if classified information is contained.
(o) Run five pages of unclassified text (font test acceptable).
(p) Destroy ribbons and clean platens.
(q) Inspect and/or test screen surface for evidence of burned-in information. If a CRT is present, it must be destroyed.

Appendix 10A. Media Destruction Log

Sample Media Destruction Log

Media Description (Include make and model if applicable.):_____

System Name: _____

Serial Number: _____

Removal From Service Date:_____

☐ For Destruction ☐ For Surplus ☐ For Reuse Disposition* (See checklist.):

Action	Completed
Remove media from operating environment and mark "Removed from Service."	☐
Store removed media in a secure location before sanitizing.	☐
Determine the disposition of the media by considering the following:	
▫ Sensitivity of data	☐
▫ Ability to render the data unreadable	☐
▫ Continued need for the media item	☐
Mark media with appropriate disposition	☐
▫ Use overwriting software on the media. *Name and version of software used:*	☐
▫ Use a degausser on media containing highly sensitive data. *Brand and coercivity of degausser used:*	☐
Verify that media is unreadable:**	☐
▫ If not unreadable, repeat degaussing.	☐
▫ If degaussing fails, mark media "For Destruction."	☐
If media is to be destroyed:	
▫ Mark "For Destruction."	☐
▫ Notify inventory representative for removal of media.	☐
If media is to be surplused:	
▫ Mark "For Surplus—Sanitized."	☐
▫ Notify inventory representative for removal of media.	☐
If media is to be reused:	
▫ Mark "For Reuse—Sanitized."	☐
▫ Return media to production environment or place in storage.	☐
Update configuration management plan.	☐
Retain the completed checklist in the sanitization log.	☐

Signature:_____ Date:_____
Verifier Signature:_____ Date:_____

** *A trained individual other than the one who performed the sanitization process should perform verification on a random basis.*

Appendix 10B. EIV Disposal Log

(Program Administrator Name)

EIV Disposal Log

Name of Employee	What was Disposed	How	Date

Appendix 11. Security Awareness Training Attendance Record

(Name of Program Administrator)

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.			
13.			
14.			

Appendix 12. Reference Listing

References:

HUD:

User Manual: Enterprise Income Verification (EIV), v 4.0, September 2005

Operations Manual: Enterprise Income Verification System (EIV), v4.0, September 2005, User Administration (Chapter 3)

This chapter discusses the administration of EIV system user functions. Topics discussed include:

- Understanding User Administration
- Searching for User Information
- User Administration-Individual User
- User Administration-Group of Users

HUD Record keeping References: Handbook No. 2225.6 REV-1, CHG-49 – HUD Records Disposition Schedules, Schedule 35, Office of Troubled Agency Recovery, Appendix 35, Nos. 69-72; Handbook 2228.1 Records Disposition Management; Handbook 2229.1 – Records Disposition Scheduling for Automated Systems

HHS:

HHS' Information Security Program, Information Security Program Handbook, November 12, 2004

HHS' Information Security Program, Information Security Program Policy, December 15, 2004