

9.0 SYSTEM ACCESS, SECURITY AND PRIVACY

Security and privacy safeguards are required throughout the development and operation of the Federal Parent Locator Service (FPLS). The purpose of this section is to summarize the controlling authority for security requirements, describe required security measures at the Federal and state levels, and highlight the Federal requirements for state system certification.

9.1 Controlling Authority for Security Requirements

Applicable Federal statutes, Office of Management and the Budget (OMB) Bulletins, Federal Information Processing Standard (FIPS) Publications, and Department of Health and Human Services (HHS) policies establish specific requirements for confidentiality, integrity and availability of information in the expanded FPLS. Safeguards that support legislation are in place to ensure the accuracy of the expanded FPLS information and to restrict access to authorized persons only, for authorized purposes. The expanded FPLS Security Plan presently under development will address these safeguards in more detail.

9.1.1 PERSONAL RESPONSIBILITY AND WORK OPPORTUNITY RECONCILIATION ACT (PRWORA) (P.L. 104-193)

PRWORA amended Title IV-D of the Social Security Act (the Act), to require the operation of the Federal Case Registry (FCR), State Case Registries (SCRs), the National Directory of New Hires (NDNH), and State Directories of New Hires (SDNHs). The Balanced Budget Act of 1997, the Taxpayers Relief Act of 1997, and the Adoption and Safe Families Act of 1997 further amended the Act, and provide additional requirements for the establishment and operation of these components of the expanded FPLS.

Section 453(m) of the Act requires the Secretary to establish and implement safeguards designed to ensure the accuracy and completeness of information in the expanded FPLS and to restrict access to confidential information to authorized persons, for authorized purposes.

Chart 1-2, “Access to FPLS Information”, which appears in Section 1.2.1, “Purpose and Objectives of the FCR”, summarizes the expanded FPLS:

1. who may request information;
2. the purposes for which the information may be requested;
3. how the information may be requested;
4. the information that may be returned; and
5. any exceptions to information disclosure.

9.1.2 FEDERAL LEGISLATIVE SECURITY REQUIREMENTS

The Social Security Act, as amended by PRWORA, contains specific references to security and privacy requirements at the Federal level.

- **§453(l)** of the Act requires that information in the FPLS, and information resulting from comparisons using such information, not be used or disclosed except as expressly provided in the Act, subject to restrictions in §6103 of the IRC of 1986.
- **§453(m)** of the Act requires the Secretary to establish and implement safeguards with respect to the entities established under PRWORA, which must be designed to:
 - ensure the accuracy and completeness of information in the Federal Parent Locator Service; and
 - restrict access to confidential information in the Federal Parent Locator Service to authorized persons, and restrict use of such information to authorized purposes.
- **§453(b)(2)** of the Act requires no information be disclosed to any person if the disclosure of such information would contravene the national policy or security interests of the United States or the confidentiality of census data. This section further requires that no information be disclosed to any person if the state has notified the Secretary that the state has reasonable evidence of domestic violence or child abuse and the disclosure of such information could be harmful to the custodial parent or the child of such parent, provided that –
 - (A) in response to a request from an authorized person (as defined in subsection (c) of this section and §463(d)(2)), the Secretary shall advise the authorized person that the Secretary has been notified that there is reasonable evidence of domestic violence or child abuse and that information can only be disclosed to a court or an agent of a court pursuant to subparagraph (B); and
 - (B) information may be disclosed to a court or an agent of a court defined in the Act as an “authorized person,” if –
 - (i) upon receipt of information from the Secretary, the court determines whether disclosure to any other person of the information could be harmful to the parent or the child; and
 - (ii) if the court determines that disclosure of such information to any other person could be harmful, the court and its agents shall not make any such disclosure.

9.1.3 THE PRIVACY ACT OF 1974 (P.L. 93-579)

The Privacy Act, 5 U.S.C. §552a, provides standards for, and restrictions on, the release of information about individuals maintained in a system of records by Federal agencies.

As the expanded FPLS will constitute a system of records in which data is retrievable by an individual’s name or SSN, the Privacy Act will govern requests for access to information in the records, including a request regarding an individual’s own record.

The Privacy Act, §552a(d) provides an individual with access to agency records that are maintained on that individual in a system of records and sets forth the responsibilities of an agency upon receipt of a request for access. Section 552a(g) establishes the civil remedies and §552a(i) the criminal penalties that may be imposed as a result of a prohibited disclosure.

9.1.4 INTERNAL REVENUE CODE OF 1986

Users of the expanded FPLS system at both the Federal and state levels need to be aware that information in the expanded FPLS that has been obtained through the Internal Revenue Service (IRS) is subject to the requirements of the Internal Revenue Code (IRC) of 1986.

The IRC §6103 establishes the confidentiality and disclosure of tax returns and return information. The IRS may disclose return information to child support enforcement (CSE) agencies. Section §6103(1)(6) of the IRC specifically details the purposes for which tax returns and return information may be used and the circumstances under which it may be used. This information may only be disclosed for the specific purpose of establishing and collecting child support obligations and for location of non-custodial parents and presumed fathers. This provision requires that tax returns and return information be confidential, and except as authorized, prohibits the disclosure of any information obtained in connection with the services of an individual who is an officer or employee of the United States, an officer or employee of any state, any local CSE agency, or any local agency administering a program who has or had access to returns or return information and any other person who has or had access to returns or return information. The term “officer or employee” includes a former officer or employee.

The IRC §7213 establishes the criminal penalties as a result of unauthorized disclosure of tax returns and return information.

Under IRC §7213A, it is unlawful for a federal or state employee to willfully inspect a tax return or return information, except as authorized by the IRC. Violations are punishable by a fine not to exceed \$1,000, or imprisonment of up to a year, or both, plus costs of prosecution. Federal employees are also subject to dismissal.

The IRC §7431 provides for civil damages against an individual personally for unauthorized inspection or disclosure of IRS information. Section §7431(c) provides for damages equal to the greater of the sum of the of \$1000 per incident of disclosure or the sum of the actual damages sustained by the person. If the disclosure was willful, or is the result of gross negligence, punitive damages may be awarded over and above the actual damages. The costs of the action may also be awarded.

9.1.5 OMB BULLETINS AND CIRCULARS

9.1.5.1 OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information

The purpose of this Bulletin is to provide guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. It requires Federal agencies to identify each computer system that contains sensitive information and to prepare and implement a plan for the security and privacy of these systems. The security planning process is designed to reduce the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information in Federal computer systems. Based upon the definition of Federal computer systems, in the Bulletin, the expanded

FPLS is a major application under development, and subject to the requirements set forth in this Bulletin.

For a review of OMB Bulletin No. 90-08, see *Instructions for Preparing System Security Plans*, which may be found on the web site <http://www.woirm.nih.gov/itmra/omb90-08.html>.

9.1.5.2 OMB Circular No. A-130, Security of Federal Automated Information Resources

Appendix III of this Circular establishes a minimum set of controls to be included in Federal automated information security programs. It also assigns Federal agency responsibilities for the security of automated information and links agency automated information security programs and agency management control systems. It further incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security directives. The expanded FPLS is a Federal information database, and must comply with the guidelines set forth. The complete Appendix III is found on website <http://csrc.nist.gov/secplcy/a130app3.txt>

9.1.6 FIPS PUBLICATIONS

FIPS Pub 73, Guidelines for Security of Computer Applications, focuses on controls for use with computer applications and provides guidance to address and prevent user access abuse and other inappropriate practices in the design, development, and operation of computer applications. The expanded FPLS is a major application under development, and as a result HHS must identify the system security objectives, degree of sensitivity, and vulnerabilities of application and its data. The expanded FPLS system is classified as Level 3 – highly critical and highly sensitive.

9.2 Expanded FPLS Federal Level Security

The expanded FPLS systems contain information that requires protection from unauthorized disclosure. The loss, misuse, unauthorized access, disclosure, or modification of expanded FPLS information could result in grave damage to the program and the privacy to which individuals are entitled under the Privacy Act of 1974. There are safeguards built in at the Federal level to ensure the privacy of FCR and NDNH data and to prevent unauthorized access to the data.

9.2.1 MANAGEMENT CONTROLS

Security for the expanded FPLS at the Federal level includes the following management controls, the development of which is evolutionary over the life of the system:

- development and implementation controls, such as design review and testing; and
- operational controls, such as emergency backup and contingency planning.

9.2.2 PHYSICAL SECURITY

The data processing for the expanded FPLS is located at the Social Security Administration's (SSA) National Computer Center (NCC). Physical and perimeter security safeguards exist to protect personnel, hardware, software, data, and other components of the NCC. Security software has been implemented to further protect the information in the expanded FPLS.

All SSA mainframes at the NCC operate under the software known as TOP SECRET Control System. TOP SECRET provides security to protect computer data from destruction, modification, disclosure, and misuse. It controls access to the computer resources and automatically logs and denies unauthorized attempts to access resources, and has the ability to log authorized use of sensitive resources for subsequent review. The SSA/OCSE administrator controls access privileges under TOP SECRET. Data transmissions from the states to the NCC are made via transmission software known as CONNECT:Direct. CONNECT:Direct uses protected, dedicated lines within SSA's closed network. The Network Control Center within the NCC employs sophisticated network monitoring software that assists in identifying unauthorized access.

9.3 State Level Security

Each state's statewide automated CSE system must be capable of exchanging information with the expanded FPLS. The Act requires that each state IV-D agency have in effect safeguards on the integrity, accuracy and completeness of, access to, and the use of data in the automated system. These safeguards are more specifically spelled out in the statewide Automated System Certification Guide. The CSE systems that receive information from the Federal database must comply with all restrictions on the use and disclosure of the information. The following provisions of the Act set out the state responsibilities regarding disclosure and access to information in the expanded FPLS.

- **§454(8)** requires the state plan for child and spousal support to provide that, for the purpose of establishing parentage, establishing, setting the amount of, modifying, or enforcing child support obligations, or making or enforcing a child custody or visitation determination, as defined in §463(d)(1) the agency administering the plan will establish a service to locate parents utilizing –
 - (A) all sources of information and available records, and
 - (B) the Federal Parent Locator Service established under §453 and shall, subject to the privacy safeguards required under paragraph (26), disclose only the information described in §453 and §463 to the authorized persons specified in such sections for the purposes specified in such sections;
- **§454(26)** requires the state plan for child and spousal support to have in effect safeguards, applicable to all confidential information handled by the state agency, that are designed to protect the privacy rights of the parties, including:
 - (A) safeguards against unauthorized use or disclosure of information relating to proceedings or actions to establish paternity, establish, modify, or to enforce support, or to make or enforce a child custody determination;

- (B) prohibitions against the release of information on the whereabouts of one party or the child to another party against whom a protective order with respect to the former party or the child has been entered;
 - (C) prohibitions against the release of information on the whereabouts of one party or the child to another person if the state has reason to believe the release of the information to that person may result in physical or emotional harm to the former party or the child;
 - (D) in cases in which the prohibitions under subparagraphs (B) and (C) apply, the requirement to notify the Secretary, for purposes of §463(b)(2), that the state has reasonable evidence of domestic violence or child abuse against a party or the child and that the disclosure of such information could be harmful to the party or the child; and
 - (E) procedures providing that when the Secretary discloses information about a parent or child to a state court or an agent of a state court described in §453(c)(2) or 463(d)(2)(B), and advises that court or agent that the Secretary has been notified there is reasonable evidence of domestic violence or child abuse pursuant to §453(b)(2), the court shall determine whether disclosure to any other person of the information received from the Secretary could be harmful to the parent or child and, if the court determines that disclosure to any other person could be harmful, the court and its agents shall not make any such disclosure.
- **§454A(d)** requires the state agency to have in effect safeguards on the integrity, accuracy, and completeness of, access to, and use of data in the automated system, which shall include the following (in addition to such other safeguards as the Secretary may specify in regulations):
 - (1) **POLICIES RESTRICTING ACCESS** – Written policies concerning access to data by state agency personnel, and sharing of data with other persons, which:
 - (A) permit access to and use of data only to the extent necessary to carry out the state program under this part; and
 - (B) specify the data which may be used for particular program purposes, and the personnel permitted access to such data.
 - (2) **SYSTEMS CONTROLS** – Systems controls (such as passwords or blocking of fields) to ensure strict adherence to the policies described in paragraph (1).
 - (3) **MONITORING OF ACCESS** – Routine monitoring of access to and use of the automated system, through methods such as audit trails and feedback mechanisms, to guard against and promptly identify unauthorized access or use.
 - (4) **TRAINING AND INFORMATION** – Procedures to ensure that all personnel (including state and local agency staff and contractors) who may have access to or be required to use confidential program data are informed of applicable requirements and penalties (including those in §6103 of the Internal Revenue Code of 1986[186]), and are adequately trained in security procedures.
 - (5) **PENALTIES** – Administrative penalties (up to and including dismissal from employment) for unauthorized access to, or disclosure or use of, confidential data.
 - **§453(b)(3)** requires the state agency to ensure that information received or transmitted pursuant to §453 is subject to the safeguards in §454(26) against unauthorized use or disclosure.

- **§453(c)** defines the term “authorized person” for purposes of making a request pursuant to §453(b) as:
 - any agent or attorney of any state having in effect a plan approved under this part [part IV-D], who has the duty or authority under such plans to seek to recover any amounts owed as child and spousal support or to seek to enforce orders providing child custody or visitation rights (including, when authorized under the state plan, any official of a political subdivision);
 - the court which has authority to issue an order against a non-custodial parent for the support and maintenance of a child, or to issue an order against a resident parent for child custody or visitation rights, or any agent of such court;
 - the resident parent, legal guardian, attorney, or agent of a child (other than a child receiving assistance under a state program funded under part A) (as determined by regulations prescribed by the Secretary) without regard to the existence of a court order against a non-custodial parent who has a duty to support and maintain any such child;
 - a state agency that is administering a program operated under a state plan under subpart 1 of part B, or a state plan approved under subpart 2 of part B or under part E.
- **§ 463(d)(2)** defines the term “authorized person” as:
 - any agent or attorney of any state having an agreement under this section, who has the duty or authority under the law of such state to enforce a child custody **or visitation** determination;
 - any court having jurisdiction to make or enforce such a child custody **or visitation** determination, or any agent of such court; and
 - any agent or attorney of the United States, or of a state having an agreement under this section, who has the duty or authority to investigate, enforce, or bring a prosecution with respect to the unlawful taking or restraint of a child.

9.4 Federal Requirements For System Certification

The Automated Systems for Child Support Enforcement: A Guide for States, developed by ACF, is designed to assist states in the development of comprehensive, statewide automated CSE systems. This guide is a tool to assist in determining the systems’ compliance with the Federal requirements for system certification. ACF retains the responsibility to monitor and evaluate programs and the automated systems, designed and developed to operate the programs, to ensure that they operate as intended by the law and regulations. OCSE AT-99-06, dated 3/25/99, which contains the Certification Guide, can be accessed on OCSE’s website at <http://www.acf.hhs.gov/programs/cse>. The guide incorporates the security requirements of PRWORA and the amendments to PRWORA as they pertain to the statewide automated system. A specific section of the Certification Guide, Section H on Security and Privacy, is the authority for the requirements for statewide automated CSE systems. This section of the Certification Guide requires the following as a prerequisite to certification of the statewide automated computer system.

9.4.1 RISK ANALYSIS

The state is required, for system certification, to ensure the following:

- Responsibility for conducting periodic risk analysis must be formally assigned.
- The risk analysis must measure the system's vulnerability to fraud or theft, loss of data, physical destruction, unauthorized access, intrusion, and harm to agency activities.
- A specific timetable for conducting a risk analysis must be established. The plan must ensure that special evaluations are performed whenever a significant change to the system's physical security, hardware or operating system software occurs.

9.4.2 SYSTEM ACCESS

The state must have policies and procedures to evaluate the system for risk on a periodic basis. The state agency is required to have in effect safeguards on the integrity, accuracy, and completeness of, access to, and use of, data in the automated system that is to include:

- written policies concerning access to data by state agency personnel, and sharing of data with other persons, which;
 - permit access to and use of data only to the extent necessary to carry out the state program; and
 - specify the data which may be used for particular program purposes, and the personnel permitted access to such data.

The statewide automated system must be protected against unauthorized access to computer resources and data in order to reduce erroneous or fraudulent activities and ensure that the privacy rights of individuals are protected against unauthorized disclosure of confidential information. The state is required, for system certification, to ensure the following:

- System, terminal, and password identifications must be controlled, randomly selected, and must uniquely identify the system user.
- Password security must extend to the functional screen level and limit the user's capability to view and/or update those screens.
- The system must automatically require the system user to change passwords periodically.
- The system must provide security levels for access to records and files and utilize automatic sign-off techniques.
- Procedures for system and terminal user identification assignment, maintenance, and cancellation must be in place.
- Delegation and maintenance of the password system must be limited to a select number of people.
- A mechanism must be in place to quickly notify those responsible for system access when there are personnel changes.
- The system must detect, record, and lock out unauthorized attempts to gain access to system software and data.
- Access to negotiable or sensitive forms must be restricted.

- IRS data, as well as FPLS data, acquired by the system must be protected from unauthorized inquiries and must be kept in a separate data file if necessary to ensure its security.
- For security purposes, the system must be capable of maintaining information on all changes to critical records and/or data fields (e.g., Arrearage Balance, Monthly Court-Ordered Support Amounts, SSN, Name, etc.) including identification of the responsible system user/caseworker and date/time of the change.
- The system must be capable of routinely monitoring the access to and use of the automated system, through methods such as audit trails and feedback mechanisms, to guard against and promptly identify unauthorized access or use.

9.4.3 SYSTEM MAINTENANCE

9.4.3.1 Application Software

The state must have procedures in place for the retrieval, maintenance, and control of the application software. The state is required, for system certification, to ensure the following:

- Change control procedures must be established to verify and validate changes to master files and application software.
- Change control procedures must ensure that only authorized changes are made to the application software and that these changes are fully tested, approved, migrated into production in a controlled manner, and documented to provide an audit trail of all system maintenance.
- Application software development must also include recovery and re-start capabilities for events such as operator errors, data errors and/or hardware/software failures.
- All testing of programs must be accomplished using test data as opposed to “live” (production) data.
- An audit trail of all operating system actions must be maintained either on the automatic console log or on the computer system’s job accounting file.
- The system must provide complete and accurate internal audit trails of all financial management activities, e.g., billing, receipting and distribution, and support order changes.
- Access to system utility programs must be limited to essential individuals with specific designation.

9.4.3.2 Program Data

The state must have procedures in place for the retrieval, maintenance, and control of program data. The state is required, for system certification, to ensure the following:

- All changes to master files must be authorized and initiated by persons independent of the data processing function.
- Override capability or bypassing of data validation on editing problems must be restricted to supervisory personnel.

- All system-generated overrides must be automatically logged by the application so that actions can be analyzed for appropriateness and correctness.
- The system must generate record counts to validate the completeness of data processed.
- All rejected data must be automatically written to a suspense file and a record count made.

9.4.3.3 System Backup/Disaster Recovery

The system hardware, software, documentation, and communications must be protected and back-ups must be available. The state is required, for system certification, to ensure the following:

- The state must have an approved disaster recovery plan which provides detailed actions to be taken in the event of a natural disaster (fire, water damage, etc.) or a disaster resulting from negligence, sabotage, mob action, etc. The disaster recovery plan should at a minimum include:
 1. documentation of approved backup arrangements;
 2. formal agreement of all parties;
 3. an established processing priority system;
 4. arrangements for use of a back-up facility; and
 5. periodic testing of the backup procedures/facility.
- The state must maintain a listing of retention periods for all application and operating system files and program versions.
- At a minimum, the state must retain off-site, in a form retrievable through automated system recovery and restore procedures, a three-year automated history of the database.
- The system must have, or be supported by, an automated recovery and restore capability in case of system malfunction or failure.
- The state must conduct routine, periodic backups of all child support system data files, application programs, and documentation.
- The state must store duplicate sets of files, programs, documentation, etc., off-site in secure, waterproof and fireproof facilities.

9.5 Consequences Of Non-Compliance

States that do not adopt security and privacy measures specified by Federal law may fail to obtain certification of their statewide automated systems. This will result in disapproval of the State Plan for child support, with a possible further consequence of reduction of Federal Financial Participation, and a reduction or loss of TANF block grant funding.

9.6 FCR To OCSE Project 1099 Interface

The FCR interfaces with the OCSE Project 1099 system. Project 1099 is a cooperative effort that involves state IV-D agencies, OCSE and the Internal Revenue Service (IRS). This project provides information to state child support enforcement agencies to assist states in their efforts to locate custodial parties (CPs), non-custodial parents (NCPs), and putative fathers (PFs) for the purpose of establishing paternity or to establish, set the amount of, or modify a child support obligation, and to enforce a child support obligation pursuant to IRS Code

§6103(1)(6). Project 1099 functionality is incorporated within the Federal Parent Locator Service (FPLS) through its Federal Case Registry (FCR) Locate processing as described in Part 6.7, “Request for Locate”.

IRS-1099 reporting forms are submitted to the IRS by certain financial institutions and state agencies for the purpose of reporting a wide variety of payments made to, or by, an individual. Information provided to states in response to a request for IRS-1099 information includes:

- the address which the CP, NCP or PF reports to the institution submitting the IRS-1099 information to the IRS;
- the address of the submitting institution; and
- asset information.

If there is a match by the IRS on the IRS-1099 Master File, states will receive address and accompanying financial information.

9.6.1 ELIGIBLE CASES, CERTIFICATION, SUBMITTING REQUESTS AND RESPONSES

Requests for IRS-1099 information may be made only for the purpose of establishing paternity or to establish, set the amount of, or modify a child support obligation, and to enforce a child support obligation pursuant to Title IV-D of the Social Security Act. Project 1099 requests are made using the “FCR Input Person/ Locate Request Record,” and responses are returned on the “FCR IRS-1099 Response Record”. See Chart G-9, “FCR Input Person/Locate Request Record – Initiate a Locate Request”, in Appendix G and Chart H-10, “FCR IRS-1099 Response Record”, in Appendix H for more detail. On a temporary basis, states may submit IRS-1099 requests that are independent of the FCR.

States must maintain strict confidentiality of information obtained through Project 1099. Therefore, in order for the FCR to process a request for IRS-1099 information for a state, the state must certify that they have established security procedures and a security system that comply with and satisfy the safeguard requirements of the Internal Revenue Code Section 6103 (p) (4). The “Sample IRS-1099 Security Agreement Letter,” which is Figure L-4 in Appendix L, “FCR Options for Data Received”, is an example of the certification each state must submit on an annual basis. If a signed certificate is not received from a state, signed by the state’s IV-D director or his designee, all requests for IRS-1099 information from that state will be denied. The signed certification must be mailed to the address shown in Appendix L, “FCR Options for Data Received”.

The IRS-1099 responses for cases on which there is a match are sent to the state on the FCR 1099 Response Record. These responses contain the following information:

- SSN, name and address of the CP, NCP, or PF;
- Account number of the CP, NCP, or PF;
- Payer’s Federal Employer Identification Number (FEIN), name and address;

- Document Code, and amount indicator, which refer to the origin and nature of the asset; and
- Amount of asset.

Asset information, as found on the IRS-1099 File, is categorized by source of assets into “document codes” and “amount indicators.”

The “FCR IRS-1099 Response Record” will indicate one of the following outcomes for each record submitted:

- 00 – Match made, the IRS financial information returned.
- 06 – Case Type changed from IV-D to Non IV-D, no information returned.
- 18 – SSN not on IRS File. No financial information returned.
- 19 – Name submitted by the state does not match with SSA name. No financial information returned.
- 20 – Information unavailable.
- 39 – Disclosure Prohibited, person associated with Family Violence.

9.6.2 VERIFICATION AND DISCLOSURE OF INFORMATION

Section 6103 (1)(6) of the Internal Revenue Code of 1986 permits the IRS to disclose return information to Federal, state and local child support enforcement agencies for the purpose of establishing paternity or to establish, set the amount of, or modify a child support obligation, and to enforce a child support obligation. The child support enforcement agency may not disclose IRS-1099 information to third parties or in litigation relating to establishing, enforcing or collecting child support obligations. However, if the information is verified by an independent source, the information from the other source may be disclosed. States must independently verify IRS-1099 information prior to disclosure and must follow all required disclosure restrictions set forth in IRS Code §6103(1)(6)(C).

9.6.3 IRS-1099 SECURITY

An essential element of Project 1099 is the safeguarding of IRS-1099 return information. While the law authorizes the IRS to disclose information to child support agencies, it also requires safeguards for and protection of, the information and provides for penalties for fraud or misuse. To review the IRS safeguarding requirements, see the Department of the Treasury, Internal Revenue Service Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies - Safeguards for Protecting Federal Tax Returns and Return Information*. The current version of this document is available on the Internet at <http://www.irs.gov/pub/irs-pdf/p1075.pdf>. This document is in a pdf file format that requires Adobe Acrobat Reader to view. Those who do not have this reader may obtain it free of charge by accessing the document on the OCSE web site and following the download instructions at <http://www.adobe.com/products/acrobat/readstep2.html>. **The IRS conducts independent security and safeguarding audits of agencies receiving IRS-1099 information.** States that do not comply with the IRS-1099 requirements risk losing their access to IRS-1099 data.

States that wish to receive IRS-1099 information must submit the “Sample IRS-1099 Security Agreement Letter”, which is Figure L-4 in Appendix L, “FCR Options for Data Received”.