SECURITY AGREEMENT

U.S. Department of Health and Human Services
Administration of Children and Families
Office of Child Support Enforcement

and

State Agency Administering the Child Support Program

I. PURPOSE AND EFFECT OF THIS SECURITY AGREEMENT

The purpose of this security agreement is to specify the management, operational and technical security controls that the state agency administering the Child Support (CS) Program shall have in place to ensure the security of Federal Parent Locator Service (FPLS) information and CS confidential program information and the information systems that transmit, store and process FPLS information and CS confidential program information.

By signing this security agreement, the state CS agency agrees to comply with the applicable security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 USC 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS) and the federal Office of Child Support Enforcement (OCSE). The state CS agency also agrees to use FPLS information and CS confidential program information solely for the authorized purposes in accordance with the terms in this security agreement between the state CS agency and OCSE. The state CS agency requests submitted to the FPLS are made solely to locate a parent for the purpose of establishing paternity, securing child support, or where applicable, to locate a parent in a parental kidnapping case, establish or enforce a child custody or visitation order, and for other purposes specified in federal law and regulations. The information exchanged between state CS agencies and all other state program information may only be used for authorized purposes under federal law and regulations (see 45 Code of Federal Regulations (CFR) 303.21) and must be protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

In this security agreement (including the addendum), "state CS agency" means the single and separate state agency responsible and accountable for the operation of the child support program under title IV-D of the Social Security Act (see 45 CFR 302.12(a)) and required to operate child support data systems under 42 U.S.C. 454(3), (24), (26), (27), and (28) as a condition of federal funding, and its agents and designees, including all of the individuals and entities described in this agreement. "Information" and "data" means all forms of confidential information or data described in this agreement.

In this security agreement (including the addendum), "State CS Director or Designee" means the

individual designated to administer the state CS program.

This security agreement is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information, and the information systems of the state CS agency, including, but not limited to, state employees and contractors working with FPLS information and CS confidential program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, and any other individual or entity collecting, storing, transmitting, or processing FPLS information and CS confidential program information.

Information originally transmitted from the FPLS to the state CS agency does not lose its character as FPLS information but remains FPLS information until its destruction; nor do the safeguarding requirements end when the information is transmitted to state CS agencies or other entities.

This security agreement is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File, and FCR are components of an automated national information system which locates employment, income, asset, and home address information on parents in child support cases for state CS agencies. The NDNH contains new hire, quarterly wage (QW), and unemployment insurance (UI) information on employees in both the public and private sector. The Debtor File contains personal information in identifiable form including names, Social Security numbers, arrearages, and other confidential information. The FCR collects and maintains records provided by state CS agency registries, which include abstracts of support orders and information from child support cases with name, Social Security number, state case identification number, state Federal Information Processing Standard (FIPS) code, county code, case type, sex, date of birth, mother's maiden name, father's name, participant type (custodial party, noncustodial parent, putative father, child), family violence indicator (domestic violence or child abuse), order indicator, locate request type, and requested locate source.

This security agreement is applicable to all CS confidential program information designated as confidential under federal law or regulation because the information relates to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. *Ref. 45 Code of Federal Regulations (CFR) 303.21(a).*

If the information system that stores, processes, and/or transmits the FPLS information and/or CS confidential program information is not under the direct management of the state CS agency, the state CS agency shall execute the attached security addendum to this security agreement. As an agent or designee of the CS agency, the organization that provides information system services to the state CS agency shall comply with all management, operational, and technical controls listed in this security agreement.

This security agreement may be updated to address changes in processes or technologies, as well as new or revised federal security requirements and guidelines. In such instances, OCSE shall

provide the state CS agency with written notification of such changes and require written assurance by the state CS agency that it shall comply with new or revised security requirements.

If OCSE determines that the security or privacy of FPLS information or any CS confidential program information is at risk, OCSE will work to support the state CS agency's efforts to provide a written description of their corrective actions or develop a Plan of Action and Milestones (POA&M) to address vulnerabilities and correct deficiencies.

This agreement shall be effective on the later of the dates on which the authorized officials of the CS agency and the agency designated to provide information services to the CS agency sign the security agreement. This security agreement shall remain in effect for a period of five years.

II. SECURITY AND PRIVACY SAFEGUARDING REQUIREMENTS

The state CS agency shall comply with the applicable provisions of the *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P)* and the *Automated Systems for Child Support Enforcement: A Guide for States*, dated August 2009 (Federal Certification Guide). The following requirements are drawn from these documents. The state CS agency was provided a copy of these documents October 2013.

The security requirements with which the state CS agency shall comply are presented in three categories: management, operational, and technical. The state CS agency shall also comply with four additional requirements: retention and disposition requirements; breach reporting and notification responsibility; security certification; and audit requirements.

A. MANAGEMENT SECURITY CONTROLS

1. The state CS agency shall establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized personnel have access to FPLS information and CS program information.

   Policy/Requirements Traceability: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations,* PL-4, PS-6, PS-8; 45 CFR 307.13(a) and (b); 45 CFR 95.621(f); 45 CFR 307.10(b)(11); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

2. The state CS agency shall advise all authorized personnel who will access FPLS information and CS confidential program information of the confidentiality of the FPLS information and CS confidential program information, the safeguards required to protect the FPLS information and CS confidential program information, and the civil and criminal sanctions for non-compliance contained in the applicable federal and state laws.

Policy/Requirements Traceability: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations,* PL-4, PS-6, PS-8; 42 U.S.C. 654 (26); 45 CFR 95.621(f); 45 CFR 307.10(b)(11); 45 CFR 307.11(b)(2)(iii); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

3. The state CS agency shall prohibit the use of non-state furnished equipment to access FPLS information and CS confidential program information without specific written authorization for use of the equipment from the appropriate state CS agency representatives.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, POES

4. The state CS agency shall require that personnel accessing FPLS information remotely, for example telecommuting, adhere to all the security and privacy safeguarding requirements provided in this security agreement. State and non-state furnished equipment shall have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Prior to electronic connection to state CS agency systems, the state CS agency shall scan the state and non-state furnished equipment to ensure compliance with a set of standards developed by the state CS agency. All connections shall be through a Network Access Control solution and all data in transit between the remote location and the state CS agency shall be encrypted using Federal Information Processing Standards (FIPS) 140-2 encryption standards. Equipment that may be authorized includes mobile devices which meet the HHS standards related to such devices. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, POES; OMB M-06-16, *Protection of Sensitive Agency Information;* OMB-M-07-16; NIST SP 800-53 Rev 3, AC-17, AC-20; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

   The state CS agency shall require that personnel accessing CS confidential program information remotely, for example telecommuting, adhere to the applicable security and privacy safeguarding requirements provided in this security agreement. State and non-state furnished equipment shall have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Prior to connection to state CS agency resources, the state CS agency shall use appropriate measures to ensure the state and non-state furnished equipment comply with a set of standards developed by the state CS agency. Equipment that may be authorized includes mobile devices which meet the state agency standards related to such devices. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, POES;

OMB M-06-16, *Protection of Sensitive Agency Information;* OMB-M-07-16; NIST SP 800-53 Rev 3, AC-17, AC-20; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

5. The state CS agency shall implement an effective continuous monitoring strategy and program to ensure the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing FPLS information and CS confidential program information.

   Policy/Requirements Traceability: NIST SP 800-53 Rev 3, CA-7; NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations;* 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H3 and H4

6. The state CS agency system shall meet all requirements set forth in the Federal Certification Guide, *Automated Systems for Child Support Enforcement: A Guide for State*, Section H, "Security and Privacy."

   Policy/Requirements Traceability: 45 CFR 302.85(a)(1); Federal Certification Guide, Chapter III, Section H, "Security and Privacy"

7. The state CS agency shall document and report to OCSE's Division of State and Tribal Systems (DSTS) any significant changes to the state CS agency's security procedures and provide copies of the appropriate updated security manual, disaster recovery plan, and risk analysis plan upon request.

   Policy/Requirements Traceability: 45 CFR 95.621(f); 45 CFR 307.13; OCSE Action Transmittal (AT)-03-03; and Federal Certification Guide, Chapter III, Sections H1, H3, H4, and H5

8. The state CS agency security office shall conduct and/or participate in the biennial system security reviews of installations involved in the administration of the state CS agency program which, at a minimum, includes evaluations of physical and data security operating procedures and personnel practices, in accordance with 45 CFR Part 95.621(f). The state CS agency shall make biennial system security reviews available to DSTS, upon request.

   Policy/Requirements Traceability: 45 CFR Part 95.621(f); and, OCSE Action Transmittal (AT)-03-03

B. OPERATIONAL SECURITY CONTROLS

1. The state CS agency shall restrict access to, and disclosure of, the FPLS information

to authorized personnel who need the FPLS information to perform their official duties in connection with the authorized purposes specified in the security agreement. The state CS agency requests submitted to the FPLS are made solely to locate a parent for the purpose of establishing parentage, or establishing, setting the amount of, modifying, or enforcing child support obligations, or where applicable, to locate a parent in a parental kidnapping case, establish or enforce a child custody or visitation order, and for other purposes specified in federal law and regulations. The information exchanged between state CS agencies shall be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

Policy/Requirements Traceability: Privacy Act 5 U.S.C. 552a (b)(1); 45 CFR 303.3(b)(6); 45 CFR 303.21; and, 45 CFR 307.13(a) and (b)

The state CS agency shall restrict access to, and disclosure of, the CS confidential program information to authorized personnel who need the CS confidential program information to perform their official duties in connection with the authorized purposes specified in the security agreement. The information exchanged between state CS agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

Policy/Requirements Traceability: 45 CFR 95.621(f)(2); CFR 303.21(a)(1); 45 CFR 307.13(a) and (b); and Federal Certification Guide, Chapter III, H2

2. The state CS agency shall label printed reports containing FPLS information and CS confidential program information to denote the level of sensitivity of the information and limitations on distribution. The state CS agency shall maintain printed reports in a locked container when not in use and never transport FPLS information and CS confidential program information off state CS agency premises unless required for a purpose approved by the state CS Director or designee. When no longer needed, in accordance with the retention and disposition requirements in section III of this security agreement, the state CS agency shall destroy printed reports by shredding or burning.

   Policy/Requirements Traceability: *HHS-OCIO Policy for Information Systems Security and Privacy (IS2P) Handbook*, MP, MS; NIST SP 800-53 Rev 3, MP-3, MP-4, MP-5, MP-6; and 45 CFR 307.13(a) and (b)

3. The state CS agency shall deliver security and privacy awareness training for authorized personnel. The training shall include information about the responsibility of such personnel for proper use and protection of FPLS information and CS confidential program information, recognizing and reporting potential indicators of insider threat, and the possible federal and state sanctions for misuse. All personnel

shall receive security and privacy awareness training prior to accessing FPLS information and CS confidential program information and at least annually thereafter. Such training shall address the federal Privacy Act and other federal and state laws governing use and misuse of FPLS information and CS confidential program information.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook,* AT; FISMA; OMB Circular A-130; OMB M-07-16; NIST SP 800-53 Rev 3, AT-2, AT-3; 42 U.S.C. 654a(d); 45 CFR 307.13(c) and (d); and Federal Certification Guide, Chapter III, H2

4. The state CS agency personnel with authorized access to the FPLS information and CS confidential program information shall sign (either in handwritten or electronic form) non-disclosure agreements, rules of behavior, or equivalent documents. The non-disclosure agreement, rules of behavior, or equivalent documents shall outline the authorized purposes for which the FPLS information and CS confidential program information may be used by the state CS agency and the federal and state civil and criminal penalties for unauthorized use.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook,* USE; OMB Circular A130, Appendix III; OMB M-07-16; NIST SP 800-53 Rev 3, PS-6; 42 U.S.C. 654a(d); 45 CFR 307.13(d); and Federal Certification Guide, Chapter III, H2

5. The state CS agency shall maintain records of authorized personnel with access to the FPLS information and CS confidential program information. The records shall contain a copy of each individual's signed non-disclosure agreement, rules of behavior or equivalent document, and proof of the individual's participation in security and privacy awareness training. The state CS agency shall make such records available to OCSE within two working days of a request for such records.

   Policy/Requirements Traceability: NIST SP 800-53 Rev 3, AT-4

6. The state CS agency shall have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving personal information), or suspected incidents involving FPLS information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state CS Director or designee shall notify the FPLS Information Systems Security Officer (ISSO) designated on this security agreement of suspected or confirmed incidents. The requirement for the state CS Director or designee to report suspected or confirmed incidents involving FPLS information to OCSE exists in addition to, not in lieu of, any state CS agency requirements to report to any other reporting agencies. The state CS Director or designee is responsible for ensuring appropriate measures are in place at the data center storing, transmitting, or processing FPLS information and to report suspected or confirmed incidents of such information to the state CS Director or designee.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, IR; OMB Circular A130, Appendix III; OMB M-07-16; NIST SP 800-53 Rev 3, IR-6; and Federal Certification Guide, Chapter III, H2

The state CS agency shall have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving personal information), or suspected incidents involving CS confidential program information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state CS Director or designee shall notify the FPLS Information Systems Security Officer (ISSO) designated on this security agreement of suspected or confirmed incidents involving 1) an unauthorized individual who obtains access, either physical or virtual, to the information systems of the state CS agency, or 2) the unauthorized disclosure or use of personal information pertaining to multiple individuals. For privacy incidents arising out of the ordinary course of business involving the unauthorized disclosure or use of CS confidential program information pertaining to one individual, the state CS director or designee must ensure prompt and adequate investigation and mitigation of the incident. The requirement for the state CS Director or designee to report suspected or confirmed incidents involving CS confidential program information to OCSE exists in addition to, and not in lieu of, any state CS agency requirements to report to any other reporting agencies. The state CS Director or designee is responsible for ensuring appropriate measures are in place at the data center storing, transmitting, or processing CS confidential program information and to report suspected or confirmed incidents of such information to the state CS Director or designee.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, IR; OMB Circular A130, Appendix III; OMB M-07-16; NIST SP 800-53 Rev 3, IR-6; and Federal Certification Guide, Chapter III, H2

7. The state CS agency shall maintain a list of personnel authorized to access facilities and systems processing sensitive data, including FPLS information and CS confidential program information. The state CS agency shall control access to facilities and systems wherever sensitive information is processed. Designated officials shall review and approve the access list and authorization credentials initially, and periodically thereafter, but no less often than annually.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, PE; NIST SP 800-53 Rev 3, AC-2, PE-2; 45 CFR 95.621(f); 45 CFR 307.13(b); and Federal Certification Guide, Chapter III, H2

8. The state CS agency shall use locks and other protective measures at all physical access points (including designated entry/exit points) to prevent unauthorized access to computer and support areas containing FPLS information and CS confidential program information.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, PE;

NIST SP 800-53 Rev 3, PE-3; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2

9. The state CS agency shall store all FPLS information and CS confidential program information provided pursuant to this security agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

   Policy/Requirements Traceability: *HHS-OCIO Policy for IS2P Handbook,* PE; NIST SP 800-53 Rev 3, PE-2, PE-3; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2

10. The state CS agency shall prohibit FPLS information from being copied to, and stored on, digital media unless encrypted at the disk or device level, using a FIPS 140-2 compliant product. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

    Policy/Requirements Traceability: *HHS OCIO Policy for IS2P* Handbook, NCRTP; OMB M-07-16; FIPS 140-2, *Security Requirements for Cryptographic Modules*; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2

    The state CS agency shall ensure that appropriate measures developed by the state CS agency are in place to protect CS confidential program information that is copied to, and stored on, digital media.

    Policy/Requirements Traceability: *HHS OCIO Policy for IS2P* Handbook, NCRTP; OMB M-07-16; FIPS 140-2, *Security Requirements for Cryptographic Modules*; 45 CFR 95.621(f); and Federal Certification Guide, Chapter III, H2

C. TECHNICAL SECURITY CONTROLS

1. The state CS agency shall utilize and maintain technological (logical) access controls that limit access to FPLS information and CS confidential program information to only those personnel who are authorized for such access based on their official duties and identified in the records maintained by the state CS agency pursuant to Section II.B.5.and II.B.7 of this security agreement.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, AC; NIST SP 800-53 Rev 3, AC-2; U.S.C. 654a(d); 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

2. The state CS agency shall prevent browsing with technical controls that limit access to FPLS information and CS confidential program information to assigned cases and areas of responsibility or equivalent compensatory controls approved in writing by OCSE.

Policy/Requirements Traceability: NIST SP 800-53 Rev 3, AC-3; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

3. The state CS agency shall transmit and store all FPLS information provided pursuant to this security agreement in a manner that safeguards the information and prohibits unauthorized access. The state CS agency and OCSE shall exchange CS confidential program information via a mutually approved and secure data transfer method which utilizes FIPS 140-2 encryption standards.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, MP; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, MP-4, SC-8, SC-9, SC-33; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

   The state CS agency shall transmit and store all CS confidential program information pursuant to this security agreement in a manner that safeguards the information and prohibits unauthorized access. The state CS agency shall use appropriate measures developed by the state CS agency when exchanging CS confidential program information among other state CS agencies.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, MP; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, MP-4, SC-8, SC-9, SC-33; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

4. Except as described in Sections II.A.4 and II.C.10 or elsewhere in this agreement, the state CS agency shall prohibit the use of digital media and computing and communications devices resident in commercial or public facilities such as hotels, convention centers, and airports from transmitting and/or storing FPLS information and CS confidential program information.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, POES; NIST SP 800-53 Rev 3, AC-19, CM-8; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

5. The state CS agency shall prohibit remote access to FPLS information, except through the use of a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication, as required by the federal Office of Management and Budget Memorandum 06-16 (OMB M-06-16). The state CS agency shall control remote access through a limited number of managed access control points. If the state CS agency cannot provide two-factor authentication, the state CS agency shall submit to OCSE a written description of compensating controls, subject to written approval by OCSE prior to allowing remote access.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, RMT,

IA; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, AC-17, IA-2, SC-8, SC-9

The state CS agency shall prohibit remote access to CS confidential program information, except through the use of appropriate measures developed by the state CS agency. The state CS agency shall control remote access through a limited number of managed access control points.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, RMT, IA; OMB M-06-16; OMB M-07-16; FIPS 140-2; NIST SP 800-53 Rev 3, AC-17, IA-2, SC-8, SC-9; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

6. The state CS agency shall utilize a time-out function for remote access and mobile devices that require a user to re-authenticate after no more than 30 minutes of inactivity. See Sections II.A.3, II.A.4, and II.C.4 of this security agreement for additional information.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, RMT; OMB M-06-16; OMB M-07-16; and Federal Certification Guide, Chapter III, H2

7. The state CS agency shall maintain a fully automated audit trail system with audit records for FPLS information that, at a minimum, collect data associated with each query transaction to its initiator, capture date and time of system events, and types of events. The audit trail system shall protect data and the audit tool from addition, modification, and/or deletion and should be regularly reviewed/analyzed for indications of inappropriate or unusual activity The state agency shall retain the audit logs for a period of five years to support security incident investigations.

   Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook*, AU; NIST SP 800-53 Rev 3, AU-2, AU-3, AU-6, AU-8, AU-9, AU-11; and Federal Certification Guide, Chapter III, Sections H2 and H3

   The state CS agency shall maintain a fully automated audit trail system with audit records for CS confidential program information that complies with provisions of the Federal Certification Guide, *Automated Systems for Child Support Enforcement: A Guide for States*, dated August 2009. The state agency shall retain the audit logs for a period of five years to support security incident investigations.

   Policy/Requirements Traceability: 42 U.S.C. 654a(d)(3); 45 CFR 95.621(f); 45 CFR 307.13(b); and Federal Certification Guide, Chapter III, Sections H2, H3 and H4

8. The state CS agency shall log each computer readable data extract (secondary store or file with duplicate CS confidential program information) from any databases holding FPLS information and verify that each extract has been erased within 90 days after completing required use. If use of the extract is still required to accomplish a purpose

authorized pursuant to this security agreement and complies with the retention and disposition requirements in Section III of this security agreement, the state CS agency shall request permission, in writing, to keep the extract for a defined period of time, subject to OCSE's written approval.

Policy/Requirements Traceability: OMB M-06-16; OMB M-07-16

The state CS agency shall use appropriate measures developed by the state CS agency to log each computer readable data extract (secondary store or file with duplicate CS program information) from any databases holding CS confidential program information and verify that each extract has been erased after completing required use.

Policy/Requirements Traceability: OMB M-06-16; OMB M-07-16; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, Sections H2, H3 and H4

9. The state CS agency shall erase electronic records after completing authorized use in accordance with the retention and disposition requirements in section III of this security agreement.

   Policy/Requirements Traceability: Privacy Act 5 U.S.C. 552a; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, Sections H2, H3 and H4

10. The state CS agency shall implement a Network Access Control (NAC) (also known as Network Admission Control) solution in conjunction with a virtual provate network (VPN) option to enforce security policy compliance on all state and non-state devices that attempt to gain access to or use FPLS information. The state CS agency shall use a NAC solution to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users before they can access the network. The NAC solution chosen or employed shall be capable of evaluating whether remote machines are compliant with security policies through host(s) Integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom-created checks tailored for the state enterprise environment. In addition, functionality that allows automatic execution of code shall be disabled. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record/report on users' access and presence on the state network. See Sections II.A.3 and II.C.4 of this security agreement for additional information.

    Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook,* S-RMT.1; NIST SP 800-53 Rev 3, AC-17, AC-20, IA-2, IA-3; and Federal Certification Guide, Chapter III, Sections H2, H3 and H4

    The state CS agency shall implement appropriate measures developed by the state CS

agency to enforce security policy compliance (such as patch level, service packs, antivirus, and personal firewall status, as well as custom-created checks tailored for the state enterprise environment) on all state and non-state devices that attempt to gain remote access to or use CS confidential program information. In addition, functionality that allows automatic execution of code shall be disabled. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record/report on users' access and presence on the state network. See Section II.A.3 and II.C.4 of this security agreement for additional information.

Policy/Requirements Traceability: *HHS OCIO Policy for IS2P Handbook,* S-RMT.1; NIST SP 800-53 Rev 3, AC-17, AC-20, IA-2, IA-3; 45 CFR 95.621(f); 45 CFR 307.13; and Federal Certification Guide, Chapter III, H2

III. RETENTION AND DISPOSITION REQUIREMENTS

The state CS agency shall erase FPLS information and CS confidential program information when data is no longer required for authorized purposes. FPLS information and CS confidential program information in an individual's case file should be safeguarded per the security requirements of this security agreement. FPLS information and CS confidential program information that is made part of an individual's case file may be retained in the individual's case file based on state CS agency's rules and procedures for case file retention.

IV. BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

Upon disclosure of FPLS information from OCSE or disclosure of CS confidential program information from another state or tribe to the state CS agency, the state CS agency is the responsible party in the event of a breach or suspected breach of the information.

Except as otherwise provided in Section II.B.6, if the state CS agency knows or suspects FPLS or CS confidential program information has been breached, in either electronic or physical form, the state CS agency:

1. Alerts the FPLS ISSO designated on this security agreement immediately upon discovery, but in no case later than one hour after discovery of the incident
2. Follows the state CS agency procedures for responding to a data breach
3. Reports the results of the investigation, mitigation, and resolution to the FPLS ISSO

The state CS Director or designee is responsible for all reporting, notification, and mitigation activities as well as the associated costs. Reporting, notification, and mitigation activities include but are not limited to: investigating the incident; communicating with required state government breach response officials; notifying individuals whose information is breached; communicating with any third parties, including the media, as necessary; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving

all issues surrounding the breach of FPLS information and CS confidential program information; performing any necessary follow-up activities to correct the vulnerability that allowed the breach; and any other activities, as required by OCSE.

The state CS Director or designee is responsible for ensuring appropriate measures are in place at the data center storing, transmitting, or processing FPLS information and CS confidential program information to report confirmed or suspected incidents of such information to the state CS Director or designee.

V. SECURITY CERTIFICATION

A. Annual Certification Statement

The state CS agency shall certify annually that it continues to comply with the terms and requirements in this security agreement by submitting a Certification Statement to OCSE each year by April 30.

B. Independent Security Assessment

Every five years, the state CS agency shall arrange for an independent security assessment to be conducted on the business processes involving FPLS information and CS confidential program information and the computer systems storing and processing FPLS information and CS confidential program information. The independent security assessment must have been conducted by an unbiased, outside entity and must include information on the management, operational, and technical security controls defined within this security agreement. The independent security assessment must also include detailed findings (if any) and recommendations to improve the state CS agency's plans, procedures, and practices. The state CS agency shall make such a report available to OCSE upon request.

The following assessments are acceptable:

- Internal Revenue Service Safeguard Review Report
- Social Security Administration Independent Validation and Verification
- A review conducted by an independent state auditing agency such as the State Office of the Inspector General
- A review conducted by an independent auditing firm hired by the state agency

The results of these independent security assessments must be incorporated into the state CS agency's respective reporting in the state's Biennial Security Review Report as required by federal regulations at 45 CFR 95.621. If major organizational, system framework, hardware, and operating software changes have taken place since the previous independent security assessment, a new independent security assessment must be conducted within six (6) months of the change. The state CS agency shall make such

reports available to OCSE, upon request.

Policy/Requirements Traceability: OMB M-11-33; OMB Circular No. A130, Appendix III; 45 CFR 95.621(f)(3) and (6); and 45 CFR 305.60

VI. AUDIT REQUIREMENTS

OCSE's Divisions of Federal Systems and State and Tribal Systems, and Office of Audit, reserve the right to audit the state CS agency or make other provisions to ensure that the state CS agency is maintaining adequate safeguards to protect the FPLS information and CS confidential program information. Audits ensure that the security policies, practices, and procedures required by OCSE are in place and to assess the completeness, authenticity, reliability, accuracy, and security of information and the systems used to process the data within the state CS agency.

Policy/Requirements Traceability: OMB M-11-33; OMB Circular No. A130, Appendix III; 45 CFR 95.621(a)(b) and (c); and, 45 CFR 305.60.

VII. PERSONS TO CONTACT

A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement security contact is:

Linda Boyer, FPLS Information System Security Officer
Division of Federal Systems
Office of Child Support Enforcement
Administration for Children and Families
370 L'Enfant Promenade, SW, 4th Floor
Washington, DC 20447
Telephone: 202-401-5410
Fax: 202-401-5558
E-mail: linda.boyer@acf.hhs.gov

B. The state CS agency program contact is:

[NAME AND TITLE]
[NAME OF DEPARTMENT]
[NAME OF PROGRAM]
[NAME OF AGENCY]
[ADDRESS OF AGENCY]
Telephone:
Fax:
E-mail:

C. The state CS agency systems contact is:

[NAME AND TITLE]
[NAME OF DEPARTMENT]
[NAME OF PROGRAM]
[NAME OF AGENCY]
[ADDRESS OF AGENCY]
Telephone:
Fax:
E-mail:

D. The state CS agency security contact is:

[NAME AND TITLE]
[NAME OF DEPARTMENT]
[NAME OF PROGRAM]
[NAME OF AGENCY]
[ADDRESS OF AGENCY]
Telephone:
Fax:
E-mail:

E. The state CS agency data center contact is:

[NAME AND TITLE]
[NAME OF DEPARTMENT]
[NAME OF PROGRAM]
[NAME OF AGENCY]
[ADDRESS OF AGENCY]
Telephone:
Fax:
E-mail:

F: The state's designated Automated Data Processing (ADP) security officer, per federal regulations at 45 CFR 95.621, is:

[NAME AND TITLE]
[NAME OF DEPARTMENT]
[NAME OF PROGRAM]
[NAME OF AGENCY]
[ADDRESS OF AGENCY]
Telephone:
Fax:
E-mail:

VIII. APPROVALS

In witness whereof, the parties hereby approve this security agreement.

A. The U.S. Department of Health and Human Services, Administration for Children and Families, Office of Child Support Enforcement Program Official

Linda Boyer	
Linda Boyer FPLS Information Systems Security Officer	**Date** 3-19-2014
Vicki Turetsky	
Vicki Turetsky Commissioner	**Date** 3-19-2014

B. State CS Director or designee (see note)

[Name of State CS Director or designee] **[Title of State CS Director or designee]**	**Date**

C. State CS agency Information Systems Security Official (see note)

[Name of State CS agency Information Systems Security Official] **[Title of State CS agency Information Systems Security Authorized Official]**	**Date**

NOTE: If the state CS director (or designee) in subsection VIII.B, or the state CS agency Information Systems Security Official in subsection VIII.C, no longer serves in the designated capacity, the individual assuming the responsibilities of either individual must sign the appropriate signature box and submit the page containing the signature to OCSE.

SECURITY ADDENDUM

State Agency Administering the Child Support Program

and

[Organization Providing Information Technology Services]

PURPOSE AND EFFECT OF THIS SECURITY ADDENDUM

The purpose of this security addendum is to affirm that any organization operating an information system that houses, processes, or transmits Federal Parent Locator Service (FPLS) information and child support (CS) program information on behalf of the state CS agency shall comply with all management, operational, and technical controls listed in the security agreement.

This security addendum is applicable to all CS confidential program information, which means confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. *Ref. 45 Code of Federal Regulations (CFR) 303.21(a)*

This security addendum is also applicable to FPLS information, which consists of the National Directory of New Hire (NDNH), Debtor File, Federal Case Registry (FCR) and all associated applications and resources. The NDNH, Debtor File, and FCR are components of an automated national information system which locates employment, income, asset, and home address information on parents in child support cases for state CS agencies. The NDNH contains new hire, quarterly wage (QW), and unemployment insurance (UI) information on employees in both the public and private sector. The Debtor File contains personal information in identifiable form including names, Social Security numbers, wages, and other private data. The FCR collects and maintains records provided by state CS registries, which include abstracts of support orders and information from child support cases with name, Social Security number, state case identification number, state Federal Information Processing Standard (FIPS) code, county code, case type, sex, date of birth, mother's maiden name, father's name, participant type (custodial party, noncustodial parent, putative father, child), family violence indicator (domestic violence or child abuse), order indicator, locate request type, and requested locate source.

Organizations to which this addendum applies include contractors of the state CS agency or other internal or external organizations working on behalf of the state CS agency.

By signing this security addendum, the state CS agency agrees to ensure that the organization providing information system services complies with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), the U.S. Department of Health and Human Services (HHS), 42 United

States Code (U.S.C.) 654(26), 42 U.S.C. 654a(d)(1)-(5) and the federal Office of Child Support Enforcement.

The organization providing information system services also agrees to protect FPLS information and CS program information against unauthorized access and to protect the privacy rights of individuals whose information is stored and processed within the information system supporting the CS program.

BREACH REPORTING AND NOTIFICATION RESPONSIBILITY

Except as otherwise provided in Section II.B.6 of the Security agreement, in the case of a confirmed or suspected data breach involving FPLS information and/or CS program information, the organization providing information system services agrees to report the breach immediately upon discovery, but in no case later than one hour after discovery of the incident, to the state CS Director or designee designated on this security addendum. See Security Agreement, Section IV for additional information.

INFORMATION SEGREGATION REQUIREMENTS

The organization providing information system services shall protect the FPLS information and state CS confidential program information and segregate it from the provider's infrastructure to ensure that only authorized personnel have access to the FPLS information and state CS program information.

AUDIT REQUIREMENTS

OCSE's Divisions of Federal Systems, State and Tribal Systems, and Office of Audit reserve the right to audit the state CS agency and any organization providing information system services to the state CS agency or make other provisions to ensure that the state CS agency is maintaining adequate safeguards to protect the FPLS information and CS program information. Audits ensure that the security policies, practices, and procedures required by OCSE are in place and to assess the completeness, authenticity, reliability, accuracy, and security of information and the systems used to process the data within the state CS agency and any organization providing information system services to the state CS agency.

Policy/Requirements Traceability: OMB M-11-33; OMB Circular No. A130, Appendix III; 45 CFR 95.621(a)(b) and (c); and 45 CFR 305.60

☐ Approved subject to and as qualified by the Plan of Action and Milestones, attached hereto and incorporated herein.

APPROVALS

In witness whereof, the parties hereby approve this security addendum.

A. State CS Director or designee (see note)

[Name of State CSDirector or designee] **[Title of State CSDirector or designee]**	**Date**

B. State CS agency Information Systems Security Official (see note)

[Name of State CS agency Information Systems Security Authorized Official] **[Title of State CS agency Information Systems Security Authorized Official]**	**Date**

C. [Organization] Information Systems Security Official (see note)

[Name of Information Systems Security Authorized Official] **[Title of Information Systems Security Authorized Official]**	**Date**

NOTE: If the state CS director (or designee) in Section A, or the state CS agency Information Systems Security Official in Section B, or the [Organization] Information Systems Security Official in Section C no longer serves in the designated capacity, the individual assuming the responsibilities of the individual must sign the appropriate signature box and have the state CS agency submit the page containing the signature to OCSE.