

March 2015

Frequently Asked Questions

1. In developing the security agreement, did the Office of Child Support Enforcement (OCSE) evaluate whether the controls required by the security agreement are consistent with Internal Revenue Service (IRS)-required controls?

Yes. Both the IRS safeguarding requirements and the OCSE security requirements are based on the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) guidance, and Office of Management and Budget (OMB) requirements.

If Child Support (CS) program information, Federal Parent Locator Service (FPLS) information, and IRS information are treated the same way, you are likely already in compliance with OCSE's security requirements.

2. Please describe why there is a distinction between FPLS and CS program information throughout the security agreement. Please also highlight the differences in safeguarding requirements for FPLS information versus CS program information.

The FPLS information is federal information and is subject to FISMA, NIST, OMB, and Department of Health and Human Services (HHS) requirements. The distinction was drawn because CS program information other than FPLS information is not subject to all of the federal requirements.

For example, in Section II.A, Management Security Control 4 requires the CS agency to have a Network Access Control (NAC) solution to access FPLS information remotely, but the CS agency decides what the requirements are for remote access to state CS information. Section IIB, Operational Security Control 1 requirements are also different for FPLS information.

3. The security agreement clearly describes FPLS information. However, CS Information is not well-defined. Please clarify the definition of CS program information.

The security agreement describes CS program information as "the state CS program information, other state and tribal program information, and confidential information."

Confidential information is further described as "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).*

March 2015

4. The agreement requires state CS agencies to undergo an independent security assessment within six months of major organizational, system framework, hardware, and operating system changes that have taken place since the previous independent assessment. Please clarify what OCSE considers a “major” change and independent security assessment. (*Section IV.B*)

We have provided several definitions of major changes, including the IRS Publication 1075 definition. State CS agencies should also review Policy Action Transmittal 06-03 Section M (August 2006) for a further description of substantive system enhancements.

We are happy to work with state CS agencies to determine if the change being contemplated would be considered “major” and would require an independent assessment.

“Best” security practices recommend a security assessment before significant changes to any environment are deployed. If the state CS agency is unable to have an independent state auditor review the new environment for little or no cost, OCSE will work with you to develop a plan that does not place additional financial burden on your agency.

From NIST 800-37 Rev. 1, F.4 Ongoing Authorization, Page F.7

Significant changes to an information system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.”

From IRS 1075, 7.1 General, Page 38:

“Significant changes would include, but are not limited to, new computer equipment, systems or applications (hardware or software); new facilities; and organizational changes such as movement to a consolidated data center from an embedded IT operation.”

The security agreement lists the following as acceptable independent assessments:

- Internal Revenue Service Safeguard Review Report;
- Social Security Administration Independent Validation and Verification;

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

- 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 CS agency.
5. The security agreement requires the state CS agency to “report to OCSE/Division of State and Tribal Systems (DSTS) any significant changes to the state CS agency’s security procedures.” Please elaborate on, or provide examples of, “significant changes” that OCSE/DSTS would require state child support agencies to report. *(Section II.A.7)*

This requirement is unchanged. The following is from the State Certification Guide section H-1:

“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.”

6. The state CS agency is required to make records of authorized personnel with access to FPLS and CS information available to OCSE, within 2 working days of a request. We would appreciate leniency on the two day turnaround for such requests. *(Section II.B.5)*

OCSE will work with you on the two day turnaround.

7. The state CS agency is required to report security or privacy incidents or suspected incidents involving FPLS or CS program information to OCSE within one hour after discovery of an incident. The state CS agency would appreciate at least 24 hours to allow sufficient time to review, investigate and notify the state IV-D Director of privacy incidents before submission to OCSE. *(Section II.B.6)*

OCSE understands that you will not have gathered all the needed information within one hour of a reported event. However, OCSE must be alerted that a potential breach has occurred because OMB requires incidents involving PII to be reported to the United States Computer Emergency Readiness Team (US CERT) within one hour. That means OCSE has to report the event through our Chief Information Security Officer to the US Department of Health and Human Services (HHS) security and privacy organization. Then, HHS must report it to US CERT. Once the initial report is completed, the state CS agency can update OCSE as information becomes available.

If the incident does not involve federal PII, we have a little more flexibility with the timeframe but still need the information as soon as the state CS agency can provide it.

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

Reference:

OMB Memorandum M-06-19 - *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*

8. The security agreement requires state CS agencies to notify OCSE of “security or privacy incidents (unauthorized disclosure of or use involving personal information).” Can OCSE provide clearer detail regarding the types of disclosures that require notification? Please also clarify if the state CS agency must notify OCSE of all incidents or if specific criterion is available in determining reportable incidents. Should the state CS agency notify OCSE of each single incident that occurs or is there a threshold or severity of incidents that must occur before submitting to OCSE? For example, does OCSE require notification if a single IV-D worker discloses FPLS or CS program information to the wrong customer not on the case? *(Section II.B.6)*

OCSE must be notified of all incidents. OMB does not make any distinction between whether it is a single incident or multiple individuals’ information has been breached. If privacy information has been breached, we must be notified.

9. The state CS agency is required to maintain a list of personnel authorized to access facilities and systems processing sensitive data including FPLS and CS program information. Does OCSE require the state IV-D office to maintain a list of personnel with access to facilities at the local offices? While we do maintain a list of personnel with access to the statewide automated system, we do not maintain a list of personnel with access to local offices. *(Section II.B.7)*

If personnel with access to local offices have access to FPLS or CS program information, whether or not they have access to the statewide system, we would expect either the state IV-D office or the local office to maintain a list. The list does not have to be maintained at the state level.

10. The security agreement requires state CS agencies to prevent browsing with technical controls that limit access to FPLS and CS program information. We interpret this requirement to be a new expansion to technical controls for CS workers. Pursuant to 45 CFR 307.13, the state agency has written policies limiting access to assigned cases or access to cases for IV-D purposes only for all personnel, including State and local staff and contractors. We anticipate this to be a significant enhancement to our systems since existing systems do not have the ability to prevent browsing. *(Section II.C.2)*

March 2015

We understand that this requires programming and will accept the compensating controls the state CS agency has in place for preventing browsing. Some examples of compensating controls could be regular audit log reviews, signed rules of behavior, and security awareness training.

11. The security agreement requires state CS agencies to log each computer readable data extract from any database holding FPLS or CS program information and erase such data within 90 days after completing required use. Please restate the requirement as it is unclear. Our interpretation requires the state or local agencies to manually and/or electronically log every occurrence of data extracted to an excel or flat file. Extraction of data is a frequent occurrence for our operations teams. Such a requirement will be a significant burden requiring additional resources to implement. *(Section II.C.8)*

This requirement is simply meant to limit databases with PII to the absolute minimum needed to perform work. A computer readable extract is a secondary store or file with duplicate data. If a state CS agency copies part or all of the FPLS data to an additional database outside of the normal process, that copy must be tracked and destroyed. The requirement is not meant to address information kept in individual client files.

The requirement is taken directly from OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

“Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required;”

12. Please consider including Tribal IV-D agencies in some way. Leaving them out will make collaboration difficult. *(Section II.B.1)*

Comprehensive tribes are mentioned in Section I page 2 which specifies “*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 program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services’ data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information.*”

13. We would prefer something like “acknowledged” to “signed” for non-disclosure agreements, rules of behavior, or equivalent documents. We manage this process

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

electronically now using the staff's user ID and password to acknowledge the document annually. (*Section II.B.5*)

The agreement has been updated to specify that the participant may sign in "handwritten or electronic form."

14. We appreciate that we can use existing reviews, such as the IRS. Will Interim Safeguard Reports suffice? (*Section V.B*)

Yes, an IRS Interim Safeguard Review Report from the IRS will suffice. Since the interim report will not contain the state CS agency responses, OCSE may request the associated Corrective Action Plan to assist with reviewing the assessment.

15. We wondered if the "never transport" applies to case files sent from one office to another location via bonded carriers for secure storage. We'd like to see such an exception as a practical matter. (*Section II.B.2*)

OCSE prefers that paper files never be transported off state CS agency premises. In those rare instances when it is deemed necessary by the state CS agency management, compensating controls such as using bonded carriers, strictly tracking the case files in transit, and verifying that the complete shipment is received will be acceptable.

16. Is the definition of remote access the same for FPLS information as it is for IRS? In the past, IRS had issues with IRS information being accessed from non-state CS agency owned computers. More recently they have accepted our situation where county attorneys access IRS information via county owned computers. They access the information via an encrypted channel. No information actually resides on the non-state CS agency owned equipment. (*Section II.A.4*)

We require remote transmission links to incorporate encryption which is compliant with the Federal Information Processing Standard (FIPS) 140-2; to utilize two factor authentication; and to be controlled by a Network Access Control (NAC) solution capable of enforcing security policy compliance on all endpoint devices used to connect to the state system housing FPLS information. As long as the state CS agency is enforcing security policy compliance, using two factor authentication, and ensuring strong encryption on transmission links, this requirement is satisfied.

17. What timeframe do states have to make the system changes needed in order to fully comply with the new FPLS security/audit requirements? Will OCSE offer a waiver or leniency while the state CS agencies make the necessary changes? For example, this section speaks to a fully automated audit trail for FPLS information which captures information on access of FPLS information. Our system does not currently

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

have this ability. I have met with System Staff who indicate this is significant, costly work effort. (*Section II.C.7*)

Building a strong security program takes time. We are certainly willing to work with you on any technical controls that are not currently implemented. That said, an audit trail is an important component of a robust security posture and the auditable items required to ensure accountability and traceability can be captured through the client/server or web-enabled applications used to access the FPLS data.

18. Does this security agreement and certification statement apply to all aspects of the FPLS State Services Portal as well? The security agreement requests us to certify that an audit trail of all searches is being maintained, but that is a federal portal. (*Section II.C.7*)

We do not expect state CS agencies to maintain an audit log of searches on the State Services Portal (SSP), but we do ask that you maintain a list of users with access to the portal. We maintain an audit trail at the federal level for all searches that come through the SSP and we review those logs regularly.

If we must research a transaction that involves the SSP, we would use a combination of our audit logs and your user list to conduct the investigation.

19. Are the regulations and controls listed in the "Policy/Requirements Traceability" section listed for reference only? Is the control in the main body text what we are being asked to implement? (*Section II*)

The Policy/Requirements Traceability information is there for reference purposes only. You are expected to comply with the control that is listed in the main body of the document.

20. May other existing audits, such as SAS-70/SOC2 and GAAP, be used to satisfy the certification requirements?

SAS-70/SOC2 will satisfy the independent assessment requirement.

The independent assessment must focus on technical, operational and management security processes and controls.

21. We have not previously been prompted to update certification documents, specifically Section H. Are we now required to re-submit Section H or are we required to certify we comply with Section H without resubmission of the actual document? (*Section V.A*)

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

The annual certification statement replaces the biennial certification statement, and state CS agencies are required to comply with the *Automated Systems for Child Support Enforcement: A Guide for States*, dated August 2009 (Federal Certification Guide).

22. Is there a template which would be used as a worksheet to track compliance with the individual components required in the security agreement and security addendum (similar to the SAR and SPR templates provided by the IRS)?

No. State CS agencies are not being asked to submit any documentation similar to the documentation the IRS requires. State CS agencies must submit the security agreement and the annual certification statement. At OCSE's request, state CS agencies will be expected to submit their most recent independent assessment and/or the State's Biennial Security Review Report.

23. Does the certification from the annual FPLS Certification Letter signed under DCL-13-18 continue on beyond December 31, 2013? Is there opportunity to phase in the requirements of Ms. Turetsky's letter dated October 21, 2013 due to the extensive review needed to ensure compliance? What is the potential impact of not meeting the December 31, 2013 deadline? (*Section V.A*)

We are willing to work with state CS agencies on a phased in approach. While these requirements are considered "best practices" and mirror some IRS requirements, we understand that state CS agencies may have to make changes to fully comply. We ask that state CS agencies provide us with the compensating controls that may be in place to mitigate the risk of non-compliance. For example, your state system may not have a fully automated audit log, but if you restrict users to specific data sets so that you are able to identify activity associated with a specific user, we would consider that a compensating control.

24. The state CS agency currently uses a reports portal to allow for easy access to electronic reports. These reports do contain FPLS data. Do electronic reports fall under this security control? (*Section II.B.10*)

Yes, electronic reports containing FPLS data are subject to section II.B.10 of the security agreement.

The state must ensure that the reports portal has applicable management, operational, and technical security controls to effectively safeguard the FPLS information and CS program information.

25. "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

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

and CS program information.” Can you define the word “prohibit” in this item and how we should go about meeting this requirement? (*Section II.C.4*)

If your state CS agency has no technical means to comply with this requirement, you can meet this requirement by issuing a policy statement that employees and contractors must not use public devices to access FPLS and CS program information.

26. “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 program information.” In using encrypted VPN tunnels for CS managers who travel around our state, will this be a violation of the prohibition? (*Section II.C.4*)

No, as long as the CS managers are using state issued or otherwise secured laptops to access the information system that houses FPLS and CS program information. There are steps your IT staff can take to ensure your CS managers’ travel safely, including using the VPN, using state issued, managed, and encrypted mobile media, using a firewall, and disabling file sharing capabilities.

27. Please clarify what is meant by Section II.C.8– is it strictly the FPLS data extracts this refers to? If so, we should be fine as X number of generations of backups are kept and it is a daily file so data would be erased before 90 days. Or does it also refer to other interfaces such as New Hire data to a system? (*Section II.C.8*)

The purpose of this control is to minimize the number of “databases” or file stores containing PII to the absolute minimum. If your process calls for duplicating all or part of the FPLS file, then you must log the duplicate file, maintain the file securely, and when it is no longer needed, you must destroy the file and record the destruction date on the log. The 90 day requirement is an OMB requirement. This control does not apply to individual case files. FPLS information in individual case files may be kept based on the state CS agency’s rules and procedures for case file retention.

28. FPLS data in the Child Support Enforcement System (CSES) is not erased or purged. FPLS data is maintained in the system unless data is overwritten by more current data. FPLS data should be maintained in CSES as it is needed for business process. Need clarification for what electronic records this includes. (*Section II.C.10*)

This control references Section III which states that “FPLS information and CS program information that is made part of an individual’s case file may be retained in the individual’s case file based on the state CS agency’s rules and procedures for case file retention.

March 2015

29. Does OCSE consider tablets (like iPads or Samsung Galaxy) to be acceptable equipment or unacceptable equipment for accessing CSE remotely? I see that PDAs, smartphones, iPods, etc. are not acceptable but I'm not clear on whether a PDA includes a tablet as they are currently available on the market or not. (*Section II.A.4*)

The reason we seem to have so many restrictions that specifically mention mobile devices is because they are attractive targets for criminals, unsecured wireless networks are easy for hackers to "eavesdrop" on, and the devices are easy to lose. But tablets are certainly acceptable for use as long as they meet the other requirements in the agreement.

Tablets such as I Pads or Samsung Galaxy must have a hardened OS and a secure network configuration in accordance with your state system security requirements. The device must be encrypted at the disk level with a FIPS 140-2 compliant product. If the device is agency owned, our assumption is that your agency has these policies in place for all mobile media. If you are allowing staff to use personally owned tablets to access FPLS or CS information, we require your security officer or other official to provide written authorization in each case. We require this authorization to be sure your agency knows that your data (and ours) is being accessed from other than state controlled devices and so that you can place restrictions on the configuration and use of those devices. Finally, we require your state to "check the health" of remote devices before they access your state resources through the use of a NAC solution. (see *Section II.A.4*)

This purpose of these controls is to protect FPLS and CS information and the system they reside upon. If your system is accessed from an insecure device that is vulnerable to intrusion, it places your state system and the data contained within it at risk. If an unencrypted tablet is lost, the FPLS or CS information on it is compromised. If the device is securely configured and fully encrypted, the data and system are protected.

30. We understand that printed reports/documents containing FPLS information must be labeled. Are there specific labels that we need to use? If so, can you please advise where we would get the labels? (*Section II.B.2*)

We suggest that you label printed reports/documents containing FPLS information to denote the level of sensitivity of the information and limitations on distribution. We do not usually provide a specific label language like "sensitive" or "confidential." So, you may use your own state CS agency language to denote the level of sensitivity of federal information being printed and stored.

31. How do I know the information I received is from the FPLS or federal information?

March 2015

If the information is provided by the FPLS, it is federal information and must be treated as such. If an employer provides the information directly to you, it is confidential but not FPLS or federal information.

32. Has OCSE provided guidance to state CS agencies on how to best implement a security and privacy awareness training program for safeguarding FTI and FPLS data? Can we combine the FTI and FPLS training or does it need to be a separate initiative? (*Section II.B.3*)

We have not offered specific guidance to the state CS agencies regarding how to best implement a security and privacy awareness training program. OCSE uses several methods (classroom and on-line training) to educate staff of the importance of protecting and safeguarding personally identifiable information. We have combined the IRS training requirements into our security and privacy training in some years and separated it in other years. It really is up to individual state CS agencies as to how it is handled. If only a small number of your staff has access to FTI, it may make sense to separate the training.

OCSE developed a web based training course for states to use about ten years ago that is still relevant and used by state CS agencies. This training would meet the requirements of the OCSE Security & Privacy Program for state CS agencies. This is the URL for the training: <http://www.acf.hhs.gov/programs/css/resource/fpls-security-awareness-training>. In addition, the IRS offers several training products for states to use. You can find them on the IRS website or in the current IRS Publication 1075.

If you would like to receive further guidance on training please reach out to us. We have a security analyst in our department who develops OCSE's training programs and also works with state agencies offering guidance as needed.

33. Does OCSE have sample language that can be used on warning banners when signing into applications containing FPLS and CS program information? (*General Comment*)

This is a sample banner with language that will meet the requirements of most government regulatory entities and addresses issues that have come up in litigation relating to unauthorized access to government-owned information technology resources. This sample can be customized to include any other warnings exclusive to your operations.

"You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on

Office of Child Support Enforcement
State Child Support Agency Security Program
Frequently Asked Questions and Comments

March 2015

this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

- *You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.*
- *Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.”*