CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES
P.O. Box 419064, Rancho Cordova, CA 95741-9064

February 6, 2015

Reason for this Transmittal

[ ] State Law, Regulation and/or Change
[ ] Federal Law, Regulation and/ or Change
[ ] Court Order or Settlement Change
[ ] Clarification requested by One or More Counties
[X] Initiated by DCSS

CSS LETTER: 15-01

ALL IV-D DIRECTORS
ALL COUNTY ADMINISTRATIVE OFFICERS
ALL BOARDS OF SUPERVISORS

SUBJECT: ON-SITE SAFEGUARD EVALUATIONS

The purpose of this letter is to inform the local child support agencies (LCSAs) that the California Department of Child Support Services (DCSS), Information Security Office (ISO), will be establishing a partnership with the LCSAs to achieve compliance through an on-site safeguard evaluation. The Internal Revenue Service (IRS) requires DCSS to conduct internal safeguard reviews every three years for LCSAs and every 18 months for data centers. This letter supersedes CSS Letter 06-17.

The evaluation will determine the adequacy of safeguards and measures employed by the LCSA to protect all child support information. The evaluation includes, but is not limited to: safeguarding of information received by the IRS, Office of Child Support Enforcement, Social Security Administration, Department of Motor Vehicles, and personally identifiable information as well as ensuring compliance with the current DCSS Information Security Manual, other state and federal policies, and information security best practices.

The DCSS ISO initiates the on-site safeguard evaluation by communication with the LCSA Director at least 30 days prior to arrival. The preliminary discussion will be followed by an electronic notification outlining the scope and purpose of the visit, a list of the specific areas to be evaluated, and staff to be interviewed.

These evaluations will not be scored or graded, nor will DCSS levy any penalties. The process will consist of an entrance and exit conference and a walkthrough of all work areas where child support information is received, processed and stored. The DCSS ISO will use the Information Compliance and Assessment Tool worksheet to document and conduct the review. The DCSS ISO may ask for additional supporting documentation. The worksheet will address the following areas:

- Record Keeping – maintain a system of records that documents the receipt, processing and storage of child support information.
- Restricted Access – care must be taken to restrict and deny unauthorized access to child support information.

- Secure Storage – security controls must be provided for a document, an item, or an area containing child support information.
- Incident Reporting – ensure that policy and procedures are in place to report security incidents or unauthorized access of child support information.
- Security Awareness – ensure employee certification of his/her understanding of agency policy and procedures for safeguarding child support information.
- Information Security – that computer security controls are in place to prevent unauthorized access to child support information.
- Disposal of Federal Tax Information – ensure destruction procedures and methods are followed.

Upon completion of the on-site evaluation, the DCSS ISO will provide a report to the LCSA Director outlining the results and will partner with the LCSA to develop an appropriate mitigation plan to address any findings.

We look forward to working together to achieve compliance in the safeguarding of all child support information. If you have any questions or concerns regarding this information, please contact the DCSS ISO at (916) 464-5045.

Sincerely,

/os/

JOHN CLEVELAND
Information Security Officer
Technology Services Division

Department of Child Support Services

On-Site Evaluations

November 20, 2014

AGENDA

- DCSS Information Security Office, DCSS-ISO Responsibilities
- Definition of FTI
- Requirements for Handling FTI
- Restrictions for Access to FTI
- On-Site Evaluation Overview

DCSS ISO Responsibilities

- DCSS ISO establishes and maintains the DCSS Security policy, standards, and guidelines, for the protection of Child Support Information, Information Systems and IT Assets used in support of the Child Support Program.
- DCSS ISO provides guidance, support and oversight for activities such as; business continuity, policy, incident, risk management, and compliance monitoring.
- DCSS ISO performs on-site evaluations to determine adequacy of physical and technical controls of all organizations within the Child Support Program including the DCSS, SDU, OSP, and LCSAs.
- DCSS ISO conducts these tasks in a professional manner that leads to superior customer satisfaction and deliver services that meet or exceed our customer's expectations.

Definition of FTI

- FTI is any Return or Return Information received directly or indirectly from the Secretary of the Treasury.
- FTI received from Office of Child Support Enforcement (OCSE) is stored in CSE.
- Most FTI provided to the child support program is received from OCSE.
- Important to Note – Return or Return information received from a NCP, CP or other participants **is not** considered FTI. This data is confidential and security controls still apply to protect it from unauthorized access.

Restrictions for Access to FTI

Access to FTI should be limited to authorized employees with a legitimate business needs.

- IRS has defined a number of physical and technical requirements that control access, even for authorized persons.
- CSE implements tracking and logging consistent with IRS requirements for information electronically stored in CSE and SDU, including the Data Repository.
- FTI received outside of CSE must be manually logged and tracked from date of receipt, during the handling, and the destruction.
- Important to Note – A manual log is required if FTI is printed, downloaded or 'saved' outside of CSE or the Data Repository.

Requirements for Handling FTI

- Every employee granted access to handle or process FTI must certify their understanding of security policy and procedure for protecting IRS information and the penalties for unauthorized disclosure. This includes contractors, consultants, and temporary employees employed by the LCSA.

- All Child Support employees at time of hire, and then annually thereafter, certify their understanding of the importance to protect child support information at all times by successful completion of the mandatory Information Security Awareness Training (ISAT) available via the Child Support University (CSU).

On-Site Evaluation Overview

What is a On-Site Evaluation?

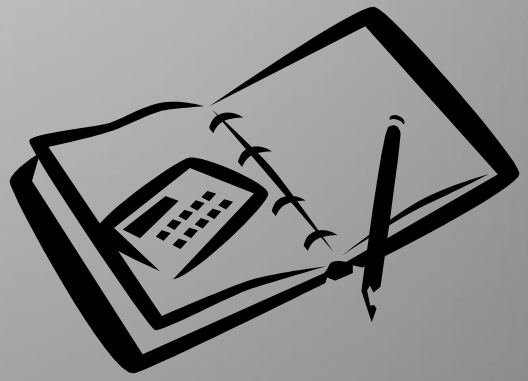
- A On-Site Evaluation is an evaluation of the use of personal, confidential, and sensitive child support information, including FTI and the measures employed to protect the data from unauthorized access.

Why On-Site Evaluations are Conducted?

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies states;
  - "As a condition of receiving FTI, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information."
  - "Agencies must ensure its safeguards will be ready for immediate implementation upon receipt of FTI."
  - "The public must maintain a high degree of confidence that the personal and financial information furnished to us is protected against unauthorized use, inspection, or disclosure."

When On-Site Evaluations are Conducted?

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies states;
  - "Agencies should establish a review cycle so that all local offices receiving FTI are reviewed within a three year cycle."
  - "Headquarters, other facilities housing FTI and the agency computer facility should be reviewed within a 18 month cycle."



On-Site Evaluation Objectives

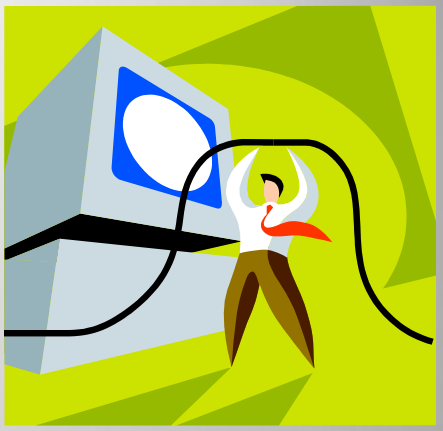
- Ensure the safeguarding of personal, confidential, and sensitive child support information, including FTI.
- Ensure compliance with DCSS ISM, NIST 800-53, Publication 1075 and CSS Letters pertaining to the safeguarding child support information and IT assets.
- Ensure IT Best Practices for privacy and security of information is followed.

On-Site Evaluation Scope

The evaluation consists of questions pertaining to the physical and technical security safeguards of personal, confidential, and sensitive Child Support Information, including FTI in the seven subject requirement areas:

- Record Keeping……..record keeping logs of FTI
- Secure Storage…building security, storage containers
- Restricting Access…..procedures to grant/limit access
- Employees Awareness……..annual security training
- Incident Reporting…….procedures to report incidents
- Disposal……..procedures to confidential destruct
- IT Security…….computer security policy/procedures

Safeguard Review Scope



Additional Requirements also cover:

- NIST SP 800-53 – which cover additional computer management, operational and technical security controls.
- DCSS Information Security Manual – compilation of departmental policies, standards and guidelines.

On-Site Evaluation Activities

- Notification letter
- Entrance conference
- On-site Evaluation
- Exit conference
- Preliminary Report
- Response and/or Plan to Address Findings
- Final Report

Proposed LCSA Schedule – 2015

- Glenn
- Yolo
- Colusa
- Sierra/Nevada
- Plumas
- Butte
- Tehama
- Sonoma
- San Francisco
- San Mateo
- Riverside
- Fresno
- Santa Cruz
- San Benito
- Monterey
- Mariposa
- Sutter
- Marin
- Lake
- Central Sierra

Questions ???????

Contact Information

DCSS – ISO
(916) 464-5045
or
Info.security@dcss.ca.gov