

**CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES**

P.O. Box 419064, Rancho Cordova, CA 95741-9064



May 31, 2013

CSS LETTER: CSS 13-01

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

SUBJECT: REVISION TO INFORMATION SECURITY MANUAL SECTION 6006

This letter revises CSS Letter 09-17, dated December 21, 2009, and updates Section 6006 – Encryption Standard of the Department of Child Support Services (DCSS), Information Security Manual (ISM) to comply with The State CIO's Technology Letter 12-15, and the most recent revision of the California State Administrative Manual as follows:

The California Child Support Program collects, stores, and processes personal and confidential information to fulfill its mission for delivery of quality child support establishment, collection and distribution of services. Pursuant to State Administration Manual (SAM) 5335.2 – Personal Computer Security, 5345.2 – Cryptography and California Civil Code 1798.29, DCSS is required to protect information in electronic form from unauthorized access. Encryption, or approved compensating security control(s) is required for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to CDs, DVDs, mainframe and server tapes, portable hard drives, and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers, netbook tablets and smart phones). All child support program information stored on tapes while in storage on or offsite or in transit must be encrypted.

DCSS must certify annually the status of our compliance with the State Information Security Office. To ensure each local child support agency has implemented the new state policy requirements, please review, sign and return the attached certification to the DCSS, Information Security Office by June 30, 2013.

If you have any questions or concerns, please contact John Cleveland, DCSS Information Security Officer at (916) 464-5774.

Sincerely,

/os/

REBECCA STILLING  
CIO/ Deputy Director

Attachment

<u>Reason for this Transmittal</u>
<input type="checkbox"/> State Law or Regulation Change
<input type="checkbox"/> Federal Law or Regulation Change
<input type="checkbox"/> Court Order or Settlement Change
<input type="checkbox"/> Clarification requested by One or More Counties
<input checked="" type="checkbox"/> Initiated by DCSS

**Local Child Support Agency (LCSA) Encryption Compliance Certification  
California Department of Child Support Services**

Date: \_\_\_\_\_

To: California Department of Child Support Services  
Information Security Office  
P.O. Box 419064, MS-10  
Rancho Cordova, California 95741-9064

Subject: ENCRYPTION COMPLIANCE CERTIFICATION

As specified in the California State Administrative Manual (SAM) 5335.2 – Personal Computer Security, 5345.2 – Cryptography and California Civil Code 1798.29, Department of Child Support Services (DCSS) is required to protect information in electronic form from unauthorized access. Encryption, or approved compensating security control(s) is required for all personal, sensitive, or confidential information that is stored on portable electronic media (including, but not limited to CDs, DVDs, mainframe and server tapes, portable hard drives, and thumb drives) and on portable computing devices (includes, but not limited to, laptop and notebook computers, netbook tablets and smart phones). All child support program information stored on tapes while in storage, on or offsite or in transit must be encrypted.

I certify that our organization is in compliance with the requirements prescribed in SAM Section 5335.2 – 5345.2 and California Civil Code 1798.29 as follows (*select one*):

Our organization complies with the policy requirements in SAM Section 5335.2-5345.2. *Information on portable electronic storage media, including mainframe and server tapes, is encrypted or is protected by approved compensating security controls.*

Our organization has NOT yet implemented all required components. We have attached our remediation plan that identifies the non-compliant components along with the timelines indicating when our organization will meet these requirements.

For additional information regarding the submission of this certification, please contact:

\_\_\_\_\_ at \_\_\_\_\_ or \_\_\_\_\_  
Name Telephone Number Email

\_\_\_\_\_ Signature of Director or Designee \_\_\_\_\_  
Printed Name of Director or Designee Date