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

Reason for this Transmittal

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

November 22, 2005

CSS LETTER: 05-34

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

SUBJECT: SUBMISSION AND MAINTENANCE OF BUSINESS CONTINUITY MANAGEMENT PLANS

REFERENCE: CSS LETTER 03-04

The purpose of this letter is to provide local child support agencies (LCSA) with direction regarding requirements for Business Continuity Management Plans (BCMP). CSS Letter 03-04, dated June 18, 2003, allowed LCSAs to either submit their current Disaster Recovery Plan or their Business Continuation Contingency Plan established for the Year 2000. In order to fully comply with federal regulations, the Department of Child Support Services (DCSS) is requesting that LCSAs submit a comprehensive BCMP by March 31, 2006. In addition, LCSAs are to provide DCSS with updates of its Key Personnel Contacts List on a semi-annual basis to ensure recovery strategies can be successfully executed.

Federal regulations (45 CFR 95 and OMB Circular A-130 Appendix III) require the establishment of policies and procedures to ensure business continuity for critical child support system functions. DCSS is responsible for overseeing the maintenance of up-to-date continuity plans for LCSAs. For the purposes of this requirement, the BCMP encompasses disaster recovery and contingency planning but does not include emergency preparedness. The BCMP refers to the process of developing advanced procedures that define how an organization will respond to an event to re-establish critical business functions. As LCSAs convert to the State Disbursement Unit, the BCMP will need to be updated to reflect the new business process. Copies of these BCMPs will be kept by DCSS in a secure library and made available to the federal Office of Child Support Enforcement as requested.

DCSS has incorporated a comprehensive guide (See Attachment) to aid in the completion of BCMPs. At a minimum, each BCMP must include the components included in the attached guide.

In order to meet the goal of having a complete, current inventory of BCMPs, LCSAs will submit updates to their original BCMP by December 31st of each year. This will include an updated Key Personnel Contacts List. If there are no changes to the BCMP on file with DCSS, the LCSA director may submit a Certification letter to Joan Obert, Deputy Director of the DCSS' Technology Services Division that will validate the accuracy of the BCMP. An update to the Key Personnel Contacts List must also be included. The following timelines have been established:

Activity	Due Date
Submission of BCMP to DCSS	March 31, 2006
Update of Key Personnel Contacts List to DCSS	June 30, 2006 and semi-annually thereafter
Submission of updates to the original BCMP or Certification and update of Key Personnel Contacts List	December 29, 2006 and each year end thereafter

BCMPs are considered confidential documents and proper measures must be taken to ensure that the confidentiality of material sent to DCSS is maintained. DCSS recommends that plans be marked confidential and be sent certified mail with a return receipt to ensure the document has been received by DCSS. Do not send plans electronically through email. DCSS will not be liable for the disclosure of confidential information if an LCSA sends a BCMP using non-secure delivery services. Please submit a hard copy of your BCMP in a three-ring binder no later than March 31, 2006 to:

California Department of Child Support Services
Technology Services Division M.S. 40
P.O. Box 419064
Rancho Cordova, CA 95741-9064

Attention: Cathy MacRae

If you have any questions or concerns regarding this process, please contact me at (916) 464-5333 or by email at joan.obert@dcss.ca.gov.

Sincerely,

/s/ Joan Obert

JOAN OBERT
Deputy Director
Technology Services Division

Attachment

Business Continuity Management Plan Guidelines

1. Assessing Business Risk and Impact of Potential Emergencies

   1.1. Emergency Incident Assessment
   This will include an examination of each potential disaster or emergency situation. The focus should be on the level of business disruption potentially likely to result from each situation. Potential emergencies include, but may not be limited to, business disruption caused by the loss of one or more of the following: environmental disasters, organized and/or deliberate disruption, loss of utilities and services, equipment or system failure, serious information security incidents.

   1.2. Business Risk Assessment
   This will include a descriptive list of the organization's key business areas. This list should be in order of importance to the business and each item should include a brief description of the business process and main dependencies on systems, communications, personnel, and information/data. It is necessary to establish standard time-bands for measuring periods when, during an emergency, normal business services could become unavailable. These time-bands are then applied to each key business process and an assessment made of the financial and operational impact for outages. For each individual key business process, it is necessary to make an assessment of the financial and operational impact of disruption to normal business operations.

   1.3. Information Technology and Communications
   This section will include a detailed specification of the main IT business processing systems and network configurations, a list of the most critical IT processes and information processing systems, a list of key IT personnel and their emergency contact information, a summary of the existing IT back-up and recovery procedures which would cover both hardware and software systems.

2. Preparing for a Possible Emergency

   2.1. Back-up and Recovery
   All LCSAs and Consortia Systems should consider what type of back-up and preventive strategies would be appropriate for each aspect of its business activities. For each key business process, determine the type of back-up process which would be appropriate. Match each key business process against the IT system and an appropriate speed of recovery strategy is chosen. Include a plan of how to continue to provide services to customers in the event of a disaster which affects either its premises or its essential equipment. Include a list of the main data and documentation used in carrying out its normal business processes; identify the potential disruption to the availability of this data and the impact of continuing a satisfactory level of business operations.

2.2. Key Personnel and Supplies

This section will contain information on who should be contacted in the event of an emergency. A functional organization chart should include the names of all key managers and staff. A list of coordinators for each functional area and a list of Key Personnel Contact Information will be included. The Key Personnel Contact list should include their position, functional area, and systems for which they are responsible. This section should include a list of key suppliers' contact information and the critical goods and/or services they supply. Include a list of Disaster Recovery Team members - specialists able to initially assist with the emergency. Personnel to consider are key members of Senior Management, Personnel Manager, Facilities Manager, Safety Officer, IT technicians, Communications technicians, Information Security Officer. Include a list of Business Recovery Team members – specialists charged with implementing the necessary recovery procedures once a serious emergency has occurred.

2.3. Key Documents and Procedures

This section should include a list of documents and records, together with a brief description, which are considered essential to the ongoing viability of the business. Emergency authorization processes need to be established to enable recovery work to proceed without unnecessary delays – this section should include information on how these emergency procedures are to operate, who is authorized to do what, and in what circumstances.

3. Disaster Recovery Phase

3.1. Planning for Handling the Emergency

During the disaster recovery process, a preliminary damage assessment as to the potential scale of the emergency from a business perspective needs to be completed. The following five point scale may be considered appropriate:

- *Is likely to seriously affect normal business operations for over four weeks;*
- *Is likely to seriously affect normal business operations between one and four weeks;*
- *Is likely to seriously affect normal business operations for over a week;*
- *Is likely to seriously affect normal business operations for less than one week;*
- *Is likely to seriously affect normal business operations for less than two days.*

3.2. Notification and Reporting During Recovery Phase

The Disaster Recovery Team Leader should initially be alerted and be responsible for notifying the rest of the Disaster Recovery Team. This section should contain a list of persons who were contacted, time and date of contact, who made the contact, instructions issued, response and subsequent time of arrival on site. It is important that all key events during the disaster recovery phase are recorded; thus, this section should include a format of an Event Log which can be maintained by the Disaster Recovery Team Leader. A copy of the log is passed on to the Business Recovery Team once the initial dangers have been controlled. On completion of the initial disaster recovery phase, the Disaster Recovery Team Leader should prepare a report which should contain information on the emergency, who was notified and when, action taken by members and outcomes arising from those actions. The

report will also contain an assessment of the impact to normal business operations.

4. Business Recovery Phase

    4.1. Managing the Business Recovery Phase
    Immediately following an emergency which seriously affects the organization's normal business processes, the Business Recovery Team (BRT) are notified and will assemble at a chosen location. The first task is the assessment of damage on the business process as opposed to the damage assessment carried out by the Disaster Recovery Team which focused on the impact on people and physical infrastructure. This section should contain a list of the areas of the business affected by the disaster and the actual business processes affected including cross dependencies of affected processes and an estimate of the recovery time involved with restoring normal operations. This section will include a Recovery Plan which will list the activities which need to be carried out in priority sequence and which persons or teams are responsible for completing those tasks. This section should include information needed for regular monitoring of progress of individual recovery tasks including milestones, dependencies, critical path, and progress reporting frequency. On completion of the Business Recovery Phase, the BRT Leader should prepare a report on activities undertaken; this section should contain a suggested format for such a report.

5. Testing the Business Recovery Process

    5.1. Planning the Tests
    This section should contain a description of the objectives and scope of the testing phase which will enable the tests to be structured and organized in a manner where the results can be measured. In setting the test environment, this section should contain a list of the conditions to be expected with each potential disruptive emergency. This section should contain a list and description of the test data needed to test recovery of each business process. This section should contain the names and duties of the members nominated to coordinate the testing process. This section will contain the names and duties of the members nominated to monitor the testing process. This section should contain a template for a Feedback Questionnaire; forms should be completed during the test or as soon after finishing, as practical.

    5.2. Conducting the Tests
    This section is to contain a list of each business process with a test schedule and information on the simulated conditions being used. The testing coordination and monitoring will endeavor to ensure that the simulated environments are maintained throughout the testing process. During the testing process, the accuracy of employee and vendor emergency contact information is to be re-confirmed. Prepare a full assessment of the test results for each business process. Each test should be assessed as either fully satisfactory, adequate, or require further testing.