

MANAGEMENT MEMO

SUBJECT: ENERGY MANAGEMENT BUSINESS CONTINUITY PLANNING AND STAGE 3 READINESS POLICY	NUMBER:
REFERENCES: GOVERNMENT CODE SECTION 11770(A)(7)	DATE ISSUED: AUGUST 22, 2001 EXPIRES: WHEN RESCINDED ISSUING AGENCY: DEPARTMENT OF INFORMATION TECHNOLOGY

Introduction

The State of California is facing an unprecedented period of electricity shortages, which presents a serious threat to government operations in the form of power outages. It is imperative that agencies/departments ensure continuity of mission-critical services during such electrical emergencies, as declared by the California Independent System Operator (CAISO), which manages the state's electrical grid. When CAISO declares a Stage 3 Electrical Emergency, state electricity-operating reserves have dropped below 1.5 percent and power outages are anticipated. The purpose of this management memo is to assist state agencies in the development or enhancement of their business continuity plans to ensure continued operation and support of mission-critical services in the event of electrical emergencies and power outages.

Under Government Code Section 11770(a)(7) the Department of Information Technology (DOIT) is mandated to "develop policies and monitor state agencies to ensure that agency business operations will continue to function in the event of a disaster." As reflected in DOIT's "Continuity Planning for Business Reference Guide" (refer to "http://www.doit.ca.gov/Reports/cpb/cpb_reference_guide.pdf"), business continuity planning focuses on providing mission-critical services to California citizens, including those involving: public safety, public health, law and justice, environmental protection, human services, and mission-critical operations.

Key considerations are as follows:

- Power outages may occur with some frequency;
- Outages may be localized or widespread;
- Outages may occur with some predictability or without advance warning; and
- Outages may be of limited duration (typically 60 to 70 minutes) or of indefinite duration.

Action

It is essential that each State agency that employs information technology (IT) in providing mission-critical services to the public consider these various scenarios in planning, communicating, and training to ensure full business continuity preparedness in the event of power outages. All plans shall be fully tested to ensure their usability in response to situations ranging from predictable rotating outages of limited duration to uncontrolled electrical grid failure.

To support business continuity planning, each agency/department must establish an energy requirements profile for critical IT equipment supporting essential agency operations and then assess the availability of alternate energy sources that can be used to power that equipment. Plans must define procedures to switch critical IT equipment over to identified alternate energy sources as well as procedures to power down any IT equipment associated with non-essential agency operations. All procedures must specify the sequence of activities and time frames required, key personnel resources, roles and responsibilities, and expected communications. In the event that alternate power supplies become unavailable, contingency procedures must be established to ensure a complete and orderly shutdown of all impacted IT equipment.

STATE ADMINISTRATIVE MANUAL

Management Memo

Page 2 of 2

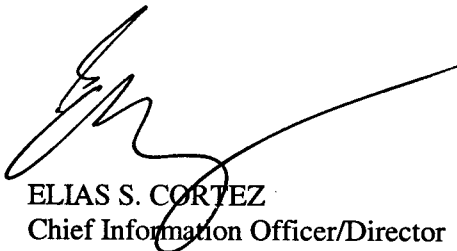
August 22, 2001

Similarly, each agency/department must define procedures for ensuring recovery to full IT operations once the outage has ended. Such procedures must address data recovery as well as equipment recovery procedures. In the event that IT equipment is damaged or becomes unusable during the course of recovery, alternate equipment must be clearly identified and available for installation.

In the event of an unforeseen electrical emergency, extended outages or alternate energy source failures may result in IT equipment becoming unavailable for extended periods of time. As a result, agency/department Business Continuity Plans should focus on alternate means of conducting business without the support of critical IT equipment. Likewise, Business Resumption Plans must ensure operations are restored to normal levels in an orderly fashion once power becomes available.

This management memo specifies that each agency/department shall review its existing Business Continuity Plan to ensure continued support of mission-critical services during electrical emergencies and provide updates as necessary. In order to fulfill its statutory requirement of monitoring statewide preparedness in ensuring continuity of critical business operations during electrical emergencies, DOIT requests that, within 30 calendar days of this management memo's publication, each agency/department either submit updated Business Continuity Plans in support of mission-critical services, or provide self-certification that no mission-critical services are provided.

The attached action plan presents short-term emergency activities that may be undertaken during the course of electrical emergencies as well as policy issues that should be addressed to ensure long-term preparedness. For further information or assistance, agencies/departments may refer to DOIT's "Continuity Planning for Business Reference Guide at http://www.doit.ca.gov/Reports/cpb/cpb_reference_guide.pdf". Additionally, agency/department Operational Recovery Plans may serve as valuable sources of information for IT inventory, key personnel, and potential areas of impact. If you have specific questions, please feel free to contact DOIT's Operational Recovery Planning Specialist at (916) 445-5900 or by e-mailing orp@doit.ca.gov.



ELIAS S. CORTEZ
Chief Information Officer/Director
State of California/Department of Information Technology

Attachment: Energy Task Force on Information Technology Stage 3 Readiness Action Plan

Energy Task Force on Information Technology
Stage 3 Readiness
Action Plan

	Standard Operations	Stage 3 (Phase 2)	Plans	Actions	Post	Funding
<u>Emergency Activities (short-term):</u>						
Update Business Continuity Plans	X		X			
Update Operational Recovery Plans	X		X			
Fully Test Plans	X		X			
Investigate Funding Sources	X		X			
		X		X	X	
Assemble Critical Personnel		X	X	X		
Open Emergency Communication Lines		X	X	X		
Prepare to Switch to Available Alternate Energy Source		X	X	X		
Power Down Non-Critical Devices		X	X	X		
Prepare for Full Shutdown		X	X	X	X	
Equipment Recovery		X	X	X	X	
Data Recovery			X			
<u>Policies (long-term):</u>						
Research Onsite Generation Alternatives			X			X
Pursue Alternative Energy Source Sources or Partnerships			X			X
High Consumption Equipment Replacement			X			X
Software Energy Management Tools			X			X
Energy Management and Monitoring Metrics			X			
Prioritize User Sites			X			
Investigate Funding Sources			X			

***Energy Task Force on Information Technology
Stage 3 Readiness
Action Plan***

Department Action Items:

- Identify alternate (backup) energy sources
- Map IT assets to critical business functions
- Prioritize and profile technology equipment energy needs (critical/non-critical)
- Assess time needed for full and partial shutdown
- Assess human resources capacity needed for full and partial shutdown
- Identify emergency communication lines
- Identify critical personnel with detailed roles and responsibilities
- Identify replacement equipment in case of key equipment failure
- Identify funding sources
- Establish and rehearse communication procedures
- Update Business Continuity Plans (cover situations of no power or no IT)
- Update Operational Recovery Plans (for rolling blackouts or complete power failure)
- Fully test Business Continuity and Operational Recovery Plans