

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

October 8, 2007

BAKERSFIELD

CHANNEL ISLANDS

CHICO

DOMINGUEZ HILLS

EAST BAY

FRESNO

FULLERTON

HUMBOLDT

LONG BEACH

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSE

SAN LUIS OBISPO

SAN MARCOS

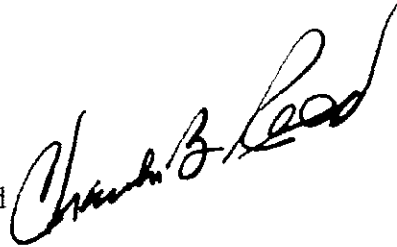
SONOMA

STANISLAUS

MEMORANDUM

TO: CSU Presidents

FROM: Charles B. Reed
Chancellor



SUBJECT: California State University Business Continuity Program -
Executive Order Number 1014

Attached is a copy of Executive Order Number 1014 relating to the California State University Business Continuity Program. This executive order delegates to each president or his/her designee, the responsibility for implementing and maintaining an ongoing program on each campus that ensures the continuity of essential functions or operations following or during the recovery phase of a catastrophic event.

In accordance with policy of the CSU, the campus president has the responsibility for implementing executive orders where applicable and for maintaining the campus repository and index for all executive orders.

If you have questions regarding this executive order, please call Ms. Charlene M. Minnick, Chief Risk Officer, Systemwide Office of Risk Management at 562-951-4580.

CBR/mas

Attachment

c: Vice Chancellors
Assistant Vice Chancellors
Executive Staff, Office of the Chancellor
Vice Presidents for Administration
Vice Presidents for Academic Affairs
Risk Managers
University Police Chiefs
Emergency Preparedness Coordinators/Managers
Environmental Health and Safety Directors
Human Resource Directors
Chief Information Officers
Information Security Officers
Chancellor's Office Divisional Heads

THE CALIFORNIA STATE UNIVERSITY
Office of the Chancellor
401 Golden Shore
Long Beach, California 90802-4210
(562) 951-4580

Executive Order: 1014
Effective Date: October 8, 2007
Title: California State University Business Continuity Program

This executive order is issued pursuant to Chapter II of the Standing Orders of the Board of Trustees of the California State University and in concert with The California Emergency Services Act in Chapter VII, commencing with Section 8550 of Division I of Title II of the Government Code.

I. Purpose

The purpose of the executive order is to maintain an ongoing program on each campus that ensures the continuity of essential functions or operations following a catastrophic event. This executive order provides guidance to the campuses for the development and implementation of business continuity plans using models such as the Continuity of Operations/Continuity of Government (COOP/COG) plans and guidelines promulgated by the California Office of Emergency Services (OES). As required by the state of California Executive Order S-04-06, all state agencies shall update their COOP/COG plans consistent with these guidelines.

II. Definitions

1. "Business Continuity" – The ability of an organization to provide service and support for its customers and to maintain its viability following a catastrophic event.
2. "Business Continuity Coordinator" – A role within the Business Continuity Program that coordinates planning and implementation for overall recovery of an organization or unit(s).
3. "Business Continuity Plan (BCP)" – Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its essential functions or operations after an interruption.

4. “Business Continuity Program” – A management framework for resuming essential functions or operations after a disaster or emergency that may threaten the health and safety of the campus community or disrupt its programs and operations.
5. “Business Impact Analysis” - A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a catastrophic event.
6. “Business Unit” – Any academic or administrative departments, unit, center, institute, division, or college.
7. “Continuity of Government (COG)” – The preservation, maintenance, or reconstitution of the institution of government. It is the ability to carry out an organization’s constitutional responsibilities. This is accomplished through succession of leadership, the pre-delegation of emergency authority and active command and control.
8. Continuity of Operations Plan (COOP)” – An effort within departments and agencies to ensure continued performance of, at a minimum, essential functions during a wide range of potential emergencies. Essentially, it is the capability of maintaining the business of government under all eventualities. This is accomplished through the development of plans, comprehensive procedures, and provisions for alternative facilities, personnel, resources, interoperable communications, and vital records/databases.
9. “Continuity of Operations/Continuity of Government Planning Program (COOP/COG)” – Developed by the California Office of Emergency Services with the goal of providing California government with the resources needed to achieve a COOP/COG capability. The program was promulgated by Executive Order S-04-06, the U.S. Department of Homeland Security - Federal Preparedness Circular #65 – Federal Executive Branch Continuity of Operations (COOP), the California State Standardized Emergency Management System (SEMS), and the National Incident Management System (NIMS).
10. “Essential Function” – Is defined in *Federal Preparedness Circular 65* as a function that enables an organization to provide vital services, exercise civil authority, maintain the safety and well being of the general public, or sustain the industrial or economic base during an emergency.
11. “Risk Assessment” - Process of identifying the risks to an organization, assessing the essential functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

12. "Training Record" - Documentation of training for employees, including employee name or other identifier, training dates, type(s) of training, training providers, and attendee sign-in sheets.

III. Responsibility

1. Campus President

The president is delegated the responsibility for the implementation and maintenance of an effective business continuity program on each campus. To facilitate oversight of the business continuity program, the president shall designate either a Business Continuity Planning Committee or a primary and secondary person with responsibility for business continuity planning activities. Such persons may be referred to as the Business Continuity Coordinator. Whether a Business Continuity Planning Committee or an individual, the president is responsible for the full outcomes of the business continuity program.

2. Business Continuity Planning Committee

If designated, a Business Continuity Planning Committee should include a cross-section of senior administrative leaders who have a working knowledge of business continuity processes and are from business units identified as key to essential operations. Such areas include, but may not be limited to, Instruction, Information Technology, Business/Financial Services, Health and Safety, and Public Safety. The president shall designate individuals to serve as the Committee Chair and Vice Chair and regular meetings should be conducted with action plans and responsibilities for campus business continuity planning activities. Meeting minutes shall be kept for a minimum of two years.

3. Business Continuity Coordinator

Working with other persons as identified by the campus, the Business Continuity Coordinator is responsible for facilitating activities that include, but are not limited to:

- A. Developing and maintaining a business continuity framework for campus business units that include policies and procedures.
- B. Establishing goals and objectives for the campus business continuity program that reflect the needs of the campus and its business units.
- C. Participating in the identification of functions and assets that are essential to operational continuity and needed to support the campus' mission.

- D. Facilitating the completion of Business Impact Analyses and Risk Assessments and development of Business Continuity Plans by business units identified as essential to operations continuity.
- E. Identifying a contact for business units and ensuring that Business Continuity Plans, Business Impact Analyses, and Risk Assessments are tested, reviewed, updated, and retained within established time periods.
- F. Recommending recovery strategies.
- G. Developing campus training and awareness and communications programs for business continuity planning.
- H. Providing independent reviews and validation of business unit continuity plans.
- I. Supporting and working with campus emergency planners and ensuring a smooth transition between emergency responders and business continuity operations personnel.

IV. **Procedures**

The campus Business Continuity Program shall include, but not be limited to, the following procedures:

1. Business Impact Analysis and Risk Assessment

Each business unit that is determined by the university to provide essential functions shall conduct a Business Impact Analysis and Risk Assessment. The Business Impact Analysis will identify essential functions and workflow; determine the qualitative and quantitative impacts of a vulnerability/threat to essential functions, prioritize/establish recovery time objectives for the essential functions, and if appropriate, establish recovery point objectives for essential functions. The Risk Assessment will identify vulnerabilities and threats that may impact the business units' ability to fulfill the mission of the campus and define the controls in place to reduce the exposure to the vulnerabilities/threats.

The Business Impact Analysis and Risk Assessment shall be approved/signed-off by the head of the business unit and the Business Continuity Coordinator or the Business Continuity Planning Committee, and retained as indicated in Section IV.F.

2. Business Continuity Plan

Each business unit that is determined by the university to provide essential functions shall develop a Business Continuity Plan that reflects sufficient forethought and detail to ensure a high probability of successful maintenance or restoration of essential functions following an unfavorable event. To assist in the accomplishment of this goal, the following elements in sample plans, including the state and federal guidance documents included in Appendix A, will be of value in developing individual department plans. Such elements include, but are not limited to:

- A. Listing and prioritization of essential functions, including the identification of staffing and resource requirements, mission critical systems and equipment, and support activities for each essential function.
- B. Lines of Succession/Delegation of Authority for key campus positions, including guidance for the delegation of emergency authorities.
- C. Alternate Operating Facilities, including provisions to sustain operations for a period of up to thirty days (or other time frame as determined by the campus)
- D. Communications, including procedures and plans for communicating with internal personnel, other agencies, and emergency personnel.
- E. Protection and safeguarding of vital records and databases.
- F. Tests, Training, and Exercises to familiarize staff members with their roles and responsibilities during an emergency, ensure that systems and equipment are maintained in a constant state of readiness, and validate certain aspects of the Business Continuity Plan.

The Business Continuity Plans shall be approved/signed-off by the head of the business unit and the Business Continuity Coordinator or the Business Continuity Planning Committee, and retained as indicated in Section IV.F. The university shall perform an administrative review of the Business Continuity Plans at least annually or more frequently as needed. The “reviewed as of date” shall appear on the plans after each review.

3. Testing and Exercising Plans

Business units shall test some part of their Business Continuity Plan once a year, with all parts tested every seven years. An actual event necessitating activation of the Business Continuity Plan will meet this requirement. At the completion of each test or review, full documentation of test results and lessons learned shall be completed in the form of a Corrective Action Plan or After Action Report. Such

reports shall be approved/signed-off by the head of the business unit and the campus Business Continuity Coordinator or the Business Continuity Planning Committee, and retained as indicated in Section IV.F. Upon request, such reports shall also be made available to the Systemwide Office of Risk Management.

4. Plan Maintenance

Business units shall review their Business Continuity Plan and tests at least annually or more frequently as needed and update the plans whenever changes occur in their operating procedures, processes, or key personnel. Plans must be updated to maintain accurate lists of key personnel, telephone numbers, and plan elements that may be affected by changes in unit structure or functions. The updated Business Continuity Plans shall be approved/signed-off by the head of the business unit and the Business Continuity Coordinator or the Business Continuity Planning Committee and retained as indicated in Section IV.F.

5. Communication

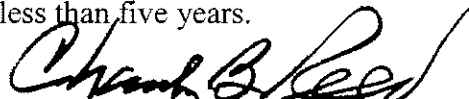
Ongoing communication of business continuity activities to the campus communities shall be provided in a variety of methods as determined by each university.

6. Training

Initial training on conducting business continuity planning shall be provided to all individuals responsible for developing and implementing plans. Additional and/or repeat training shall be provided as determined necessary by the Business Continuity Coordinator or the Business Continuity Planning Committee following the review of written plans and plan testing.

7. Record Retention

The campus shall retain business continuity records, including those indicated in Section IV.A through D, for a period of not less than five years.


Charles B. Reed, Chancellor

Dated: October 8, 2007

OPERATIONS/CONTINUITY OF GOVERNMENT PLAN (COOP/COG)

This guidance is based upon guidance from the *Department of Homeland Security (DHS) Headquarters Continuity of Operations (COOP) Guidance Document, dated April 2004* and the sample Concept of Operations (COOP) template developed by the Federal Emergency Management Agency (FEMA). It can be used as the basic foundation for Continuity of Operations/Continuity of Government (COOP/COG) Plans for State of California, Executive Branch agencies. Organizations are encouraged to tailor COOP/COG Plan development to meet their own needs and requirements. Organizations should include any additional elements that are helpful to understanding and implementing their COOP/COG Plan. The result will be a baseline plan that can be refined and enhanced over time.

I. EXECUTIVE SUMMARY

The executive summary should provide a brief overview of the overall COOP/COG Program, including policies, plans, processes, materials, and activities that support the organization's COOP/COG capability. It should briefly outline the organization and content of the COOP/COG Plan and describe what it is, whom it affects, and the circumstances under which it should be executed. Further, it should briefly discuss the key elements of COOP/COG Planning and explain the organization's implementation strategies.

II. INTRODUCTION

The introduction to the COOP/COG Plan should explain the importance of COOP/COG Planning to the organizations. COOP/COG Plans address incidents that disrupt normal operations. They are needed to address exceptional and adverse operating conditions. The introduction should include typical adverse conditions anticipated to be covered by the COOP/COG Plan. The introduction should also discuss the background behind continuity planning and may reference recent events that have led to the increased emphasis on the importance of a COOP/COG business continuity capability for the organization. It should explain the intended use of the document and the plan's architecture (e.g., how the COOP/COG Plan is organized and where information is housed).

III. PURPOSE & ASSUMPTIONS

A. PURPOSE

The purpose section should briefly discuss applicable Federal and State guidance, affirm the organization's commitment to COOP/COG planning, and explains the overall purpose of COOP/COG planning, which is to ensure the continuity of mission essential functions. The purpose section should also explain that the plan identifies recovery strategies for essential functions. Although there may be other

important functions, this plan only covers those that are mission and time critical. A definition of essential function is useful to include here. An Essential Function is defined in the *Federal Preparedness Circular 65* as a function that enables an organization to:

1. Provide vital or “mission critical” services;
2. Exercise civil authority;
3. Maintain the safety of the general public; or
4. Sustain the industrial or economic base during an emergency.

This section should also explain how the organization’s essential functions are prioritized. These priority classifications are based on recovery time objectives (RTOs). An RTO is an estimate of the maximum tolerable duration between when a disruption occurs and when the function is resumed under emergency conditions (e.g., the maximum amount of time the function can be down). The following classification system was used by OES to prioritize its essential functions and is included only as an example. An organization may choose different priority classifications based on their responsibilities and essential functions:

- a. Emergency response functions (0-2 hours)
- b. High impact on public health or safety (up to 24 hours)
- c. High impact on public safety and health, or on department critical operations (up to 72 hours)
- d. Moderate impact on public safety, health or department critical operations (1-3 weeks)
- e. Low impact (3 weeks or longer)

Organizations can elect to use alternate criteria to determine the recovery priorities for its essential functions. Organizations should avoid using rank-ordering priority methods during the continuity process, since some essential functions may be equally important to the organization and have similar recovery time objectives.

B. ASSUMPTIONS

This section should include the assumptions on which the COOP/COG Plan is based. Each COOP/COG Plan is based on a set of assumptions that, if not true, will render the plan ineffective. The test for a planning assumption is: will the plan fail if the assumption is not true? A sample set of basic assumptions may include: (1) emergencies or threatened emergencies may adversely affect the organization’s ability to continue to support essential internal operations and to provide services to clients or support to external agencies, and (2) personnel and other resources from the organization and other organizations outside of the area

affected by the emergency or threat will be made available if required to continue essential operations.

IV. APPLICABILITY AND SCOPE

A. APPLICABILITY

This section should describe the applicability of the COOP/COG Plan to the agency as a whole, as well as to specific personnel and groups within the organization. Additionally, this section should describe the role of other plans and their relationship to the organization's COOP/COG Plan. Other planning documents may include Operational Recovery Plans (ORPs), Emergency Operations Plans (EOPs), and Disaster Recovery Plans (DRPs). This section should distinguish COOP/COG Plan capabilities from these other plans and address specific contingency plans for particular risks that might be contained in this COOP/COG Plan.

B. SCOPE

This section should include the scope and limitations of the plan. COOP/COG Plans should strive to map out the restoration of normal operations and failed facilities or equipment with a skeletal crew and minimum resources needed to achieve this task. This section provides the focus for the planning efforts. The plan's scope should encompass all of the organization's essential functions and must be based on the "worse case scenario" which would include the inaccessibility or unavailability of the organization's facility of building complex, and all of its contents. You should consider the division, business units, and essential functions covered by the COOP/COG Plan, the anticipated response time required to recover essential functions under emergency circumstances, and the period of sustainment.

This section should also include the organization's specifications regarding plan performance. For example, the organization expects a response time of 24-hours for all essential functions identified in the plan and a sustainment period of 30 days for those functions. Other specifications may include that the plan addresses emergencies that occur both with or without warning, or during on-duty or off-duty hours.

Limitations that are included in this section may include scenarios that this COOP/COG Plan are not contemplated to cover or vulnerabilities that have been identified during the planning process for which solutions are not yet available.

V. ESSENTIAL FUNCTIONS

The identification of essential functions is a prerequisite for all COOP/COG Planning. It establishes the parameters that drive the organization's continuity planning efforts. In this section or in an annex, you should include a complete list of the organization's

prioritized essential functions. Essential functions are organizational functions and activities that must be continued under any and all circumstances. The list should be based on the prioritization strategy introduced in **Section III-A: Purpose**.

A. RISK ANALYSIS

A risk analysis is the process of collecting and evaluating information on risks and hazards that may impact the organization's operations. Risks can typically be categorized into three groups:

1. Natural hazards, such as floods, earthquakes, fires, severe weather, and public health emergencies (e.g., Pandemic Flu);
2. Human-related hazards, or technological events (e.g., power outage, communication outage);
3. Pro-active human hazards, sometimes called **threats**, reflecting deliberate actions by individuals or groups to cause harm, such as workplace violence, bomb threats, and civil disturbances.

In this section, the organization should identify possible risks or hazards that may threaten the continuance of essential functions. The purpose of the risk analysis is to develop a list of hazards that are of such significance that they are reasonably likely to cause devastating harm to the agency if they are not effectively controlled. The objective of this analysis is to identify vulnerabilities in operations and take steps to mitigate losses and/or develop recovery strategies.

To complete a risk analysis, the organization should:

1. List all the threats that may potentially have an impact on the organization's ability to deliver its essential functions.
2. Assess the impact of the risk based on the severity of the impact of the threat and the probability of occurrence.
3. Assess whether the organization has implemented effective control measure or other procedures that mitigate the occurrence of loss or damage resulting from this event.
4. Determine if the likelihood or occurrence of this threat is substantial enough to be included in the organization's COOP/COG Plan.

B. VULNERABILITY ASSESSMENT

In this section, the organization should provide a vulnerability assessment for each essential function. This assessment should identify scenarios that pose a risk

to the continuity of the function. In COOP/COG planning, the planning can become extremely cumbersome if specific plans were to be developed for every possible type and circumstance of something going wrong.

This first step in preparing a vulnerability assessment is to survey or scan the environment of possible risks identified above and translate that environment into a set of risk scenarios.

For most operations, the following scenarios have proven to be sufficient:

1. Local facility disruptions, typically single buildings;
2. Region-wide disruptions affecting all or many government buildings in the region;
3. Disruption of a communications system;
4. Disruption of access to vital records or databases;
5. Disruption to availability of specialized equipment or systems, including computing systems (other than traditional communications systems);
6. Loss of services from a vendor or another government agency;
7. Unavailability of personnel.

In the second step, determine whether your organization has existing capabilities to recover the essential function if the resources were lost for areas where a disruption may have major or significant impact on operations. Consider formal processes that are currently in place for recovering operations. These formal processes or “standard operating procedure” should become part of the COOP/COG Plan. The existence of the capability should be noted because it enhances awareness of how resiliency of operations is ensured. Those areas where existing capabilities do not exist to recover the essential function are identified as vulnerabilities.

C. RESOURCE REQUIREMENTS

In this section, the organization should evaluate the resources that are needed to continue certain essential functions during an emergency. These resources include:

- Facilities or Work Sites
- Communication Systems
- Key Personnel
- Vital Records and Databases
- Vital Systems and Equipment
- Key Vendors
- Supporting Government Agencies or Departments

The organization should identify the minimum resource requirements needed to support each essential function. After these resources have been identified, the organization can work towards ensuring that the resources are protected at all times. For those resources that cannot be adequately safeguarded, the organization must select alternate or back-up resources in order to ensure that essential functions are available at all times.

D. FUNCTION DEPENDENCIES

Many of the organization's essential functions may rely on the availability of resources or functions controlled by another organization, including other agencies: federal, state and/or local governments; and private entities. In this section, organizations should identify these dependencies and link them to the essential function(s) that they support. The required recovery time objective (RTO) for each of these dependencies should be identified and indicate whether the organization is satisfied with the level of support or if this dependency represents a vulnerability.

V. AUTHORITIES AND REFERENCES

This section should reference an annex that outlines all supporting authorities and references that have assisted in the development of the COOP/COG Plan. This section should also include any federal, state, or local ordinances that allow for the designation of emergency or temporary locations for the seat of government, or the actions required to transition the affairs of state government. In addition, it should include any specific provisions that allow for the delegation of authority.

VI. CONCEPT OF OPERATIONS

This section should briefly explain how the organization will implement its COOP/COG Plan, and specifically, how it plans to address each critical COOP/COG element. This section should be separated into three phases: activation and relocation, alternate facility operations, and reconstitution. Organizations should also develop an executive decision process that would allow for a review of the nature and extent of the emergency to determine the best course of action for response and recovery. This process will preclude premature or inappropriate activation of an organization's COOP/COG Plan.

A. PHASE 1: ACTIVATION AND RELOCATION

The Phase I section should explain COOP/COG Plan activation procedures and relocation procedures from the primary facility to the alternate facility. This section should also address procedures and guidance for non-relocating personnel.

1. Decision Process

This section should explain the logical steps associated with implementing a COOP/COG Plan, the general incident escalation process, the circumstances under which a plan may be activated (both with and without warning), and should identify who has the authority to activate the COOP/COG Plan. This process can be described here or depicted in a graphical representation. This section should also include a brief description of the organizational structure of the response teams, including the COOP/COG Initial Assessment Team, the COOP/COG Executive Command Team, and the Essential Function Recovery Teams. The roles and responsibilities of each team should be explained in this section.

2. Alert, Notification, and Implementation Process

This section should explain the events following a decision to activate the COOP/COG Plan. This includes employee alert and notification procedures and the COOP/COG Plan implementation process. Any tools used in the alert and notification process, such as notification trees or automated software should be noted in this section.

3. Leadership

a. Lines of Succession

This section should identify lines of succession to key positions within the organization. The lines of succession should be of sufficient depth to ensure the organization's ability to manage and direct its essential functions and operations (at least three deep). The conditions under which succession will take place, the method of notification, and any temporal, geographical, or organizational limitations of authority should also be identified in this section. You should identify any existing statutes covering lines of succession.

b. Delegations of Authority

This section should identify, by position, the authorities for making policy determinations and decisions at headquarters, field levels, and other organizational locations, as appropriate. Generally, pre-determined delegations of authority will take effect when normal channels of direction are disrupted and terminate when these channels have resumed. Such delegations may also be used to address specific competency requirements related to one or more essential functions that are not otherwise satisfied by the lines of succession. Delegations of authority should document the legal authority for making key decisions, identify the programs and administrative authorities

needed for effective operations, and establish capabilities to restore authorities upon termination of the event.

c. Devolution

The devolution section should address how the organization will identify and conduct its essential functions in the aftermath of a worst-case scenario, one in which the leadership is incapacitated. The organization should be prepared to transfer all of their essential functions and responsibilities to personnel at a different office or location. You should identify any provisions, if any, for pursuing devolution and include a list of alternative agencies.

4. Relocation

This section should include procedures for relocating essential functions, including required resources, to an alternate facility. This section should also include procedures for dealing with personnel who are not to be relocated to the alternate facility. If an organization has existing emergency relocation plans, they may be incorporated by reference.

B. PHASE II: ALTERNATE FACILITY OPERATIONS & RECOVERY STRATEGIES

The Phase II section should identify initial arrival procedures, as well as operational procedures, for the continuation of essential functions at an alternative facility.

1. Alternate Locations

In the event of an emergency, identifying an alternate facility capable of supporting essential operations, positions, and personnel is critical. These facilities must be capable of supporting operations in a threat-free environment, as determined by the geographical location of the facility and the collective protective characteristics of the facility.

This section should include a list of alternate facilities to which essential functions will be relocated and the resources that are required to be available at the alternate location. In this section, you should identify existing alternate locations that have been identified, including memorandums of understanding. This section should include strategies for moving and recovering essential functions at the alternate location, including the pre-positioning of supplies, mirroring computer systems and databases at the alternate facility, or putting service level agreements in place with key vendors.

2. Mission Critical Systems & Equipment

The section should address the organization's mission critical systems and equipment necessary to perform essential functions and activities.

Organizations must define these systems and equipment and address the method of transferring/replicating them at an alternate site.

3. Vital Files, Records, and Databases

This section should address the organization's vital files, records, and databases, to include classified or sensitive data, which are necessary to perform essential functions and activities and to reconstitute normal operations after the emergency ceases. Organizational elements should preposition and update on a regular basis those duplicate records, databases, or back-up electronic media necessary for operations.

There are three categories of records to be reviewed and prioritized, then transferred (either hard copy or electronic media) to an alternate location:

- a. Emergency operations records;
- b. Legal/financial records; and,
- c. Records used to perform state or national security preparedness functions and activities.

4. Interoperable Communications

This section should address the organization's mission critical communication systems necessary to perform essential functions and activities. Organizations must define these systems and address the method of transferring/replicating them at an alternate site. This section should address both operable and interoperable communications, which includes equipment with voice and/or text capability. Examples of such equipment include the following:

- Mobile Telephones
- Satellite Telephones
- Blackberries
- Two-way radios
- Pagers
- Non-secure Telephones
- Secure Telephones
- Internet connection for email and web access
- Facsimile

5. Human Capital (Protection of Government Resources -- Specifically Personnel)

In this section, the organization should list existing procedures that are in place to protect an organization's resources, with an emphasis on personnel. This section should specify the resources and personnel to be transferred to the alternate site and the methods for safely transporting them to the site. It

should also describe the various documents and checklists available to employees to encourage and facilitate individual and family preparedness.

6. Vendors & Other Agency Functions

In this section, the organization should identify how it will continue to receive needed support from external vendors or supporting agencies at the alternate site.

C. PHASE III: RECONSTITUTION & RESUMPTION STRATEGIES

The Phase III section should explain the procedures for resuming normal operations – a time phased approach may be most appropriate. This section may include procedures for returning to the primary facility, if available, or procedures for acquiring a new facility. Notification procedures for all employees returning to work must also be addressed. Organizations should also anticipate developing an After Action Report (AAR) to determine the effectiveness of COOP/COG plans and procedures.

VIII. COOP/COG PLANNING RESPONSIBILITIES

This section should include additional delineation of COOP/COG responsibilities of each key staff position, to include members of the COOP/COG Senior Activation Team or Crisis Management Team, and possibly an Essential Function Recovery Team. Team members and individuals should be identified in the order of succession and delegation of authority. This section should also include responsibilities for the COOP/COG Planners responsible for normal day-to-day program support.

IX. LOGISTICS

This section of the COOP/COG Plan should contain information about recovery logistics requirements. Examples of these requirements include:

- ❑ Space requirements;
- ❑ Human Support Requirements, such as food provisions, sleeping arrangements, transportation, etc.; and
- ❑ Memorandums of Understanding and Provisioning Contracts (the actual documents may be housed in annexes).

This section should also include detailed recovery procedures for the loss of key resources. Much of the information contained in this section will actually be owned by division representatives rather than the COOP/COG Program. The plan itself may contain references to where this information is housed and maintained within the organization.

A. ALTERNATE LOCATION

The alternate location section should explain the significance of identifying an alternate facility, the requirements for determining an alternate facility, and the advantages and disadvantages of each location. Senior managers should take into consideration the operational risk associated with each facility. Performance of a

risk assessment is vital in determining which alternate location will best satisfy an organization's requirements. Alternate facilities should provide:

1. Sufficient space and equipment;
2. Capability to perform essential functions within 12 hours, up to 30 days (or other time frame as determined by the organization);
3. Reliable logistical support, services, and infrastructure systems;
4. Consideration for health, safety, and emotional well-being of personnel;
5. Interoperable communications; and
6. Computer equipment and software.

B. MISSION CRITICAL SYSTEMS & EQUIPMENT

The mission critical systems and equipment section should identify available and redundant mission critical systems and equipment that are located at the alternate facility. These systems and equipment should provide the organization with the ability to perform its essential functions at the alternate facility, as well as to support the organization's resumption to normal operations. Mission critical systems and equipment should provide:

1. Capability commensurate with an organization's essential functions;
2. Ability for personnel to access systems and equipment;
3. Ability to support COOP/COG operational requirements; and
4. Ability to operate at the alternate facility within 12 hours and for up to 30 days (or the time frame determined by the organization).

C. INTEROPERABLE COMMUNICATIONS

The interoperable communications section should identify available and redundant critical communication systems that are located at the alternate facility. These systems should provide the ability to communicate within the organization and outside the organization. Interoperable communications should provide:

1. Capability commensurate with an organization's essential functions;
2. Ability to communicate with essential personnel;
3. Ability to communicate with other agencies, organizations, and customers;
4. Access to data and systems;
5. Communication systems for use in situations with and without warning;
6. Ability to support COOP/COG operational requirements;
7. Ability to operate at the alternate facility within 12 hours and for up to 30 days (or the time frame determined by the organization); and
8. Interoperability with existing field infrastructures.

D. PERSONNEL

This section should identify personnel with key skills or experience and available back-up resources. When identifying key personnel, consider the following circumstances:

1. Specialized training or skills that are required to perform the essential function;
2. The minimum number of personnel required to perform the essential function;
3. Other personnel available with skills that are transferable to support essential functions; and
4. Whether performance of the essential function requires transfer of the personnel to an alternate site (i.e., personnel can perform tasks via telecommuting).

E. VENDORS & OTHER AGENCY FUNCTIONS

This section should identify the availability of vendors or other agencies to support essential functions. This section should identify the procedures to be used for the delivery of services at the alternate facility.

X. TEST, TRAINING, AND EXERCISES

This section should address the organization's Test, Training, and Exercise (TT&E) Plan. Tests, Training, and Exercises familiarize staff members with their roles and responsibilities during an emergency, ensure that systems and equipment are maintained in a constant state of readiness, and validate certain aspects of the COOP/COG Plan. Managers may be creative when it comes to COOP/COG readiness and include snow days, power outages, server crashes, and other ad-hoc opportunities to assess preparedness.

To maximize the capabilities of potential responders, all employees should participate in the planning, implementation, and critique of exercises that test their COOP/COG plan. Testing the COOP/COG Plan will validate the plans, policies, procedures and systems; identify deficiencies in the COOP Plan and allow for subsequent correction.

The TT&E plans should provide:

1. Individual and team training of organization personnel;
2. Internal organization testing and exercising of COOP/COG plans and procedures;
3. Testing of alert and notification procedures;
4. Refresher orientation for COOP/COG personnel; and
5. Joint interagency exercising of COOP/COG plans, if appropriate (for example, situations where an organization's ability to deliver an essential function is dependent on a support function from another organization).

The effectiveness of the training exercises should be documented in a Post Exercise Assessment, which should be prepared within one to two weeks of the exercise, while memories are still fresh.

XI. MULTI-YEAR STRATEGY PROGRAM MANAGEMENT PLAN & BUDGET

A comprehensive COOP/COG plan is often the result of layer after layer of development over time. Initially, an organization should focus on establishing a baseline of capability for each of the eleven COOP/COG elements. The organization should document where there continue to be gaps in their preparedness and develop a plan/strategy for addressing them. This is often captured in a Multi-Year Strategy Program Management Plan (MYSPMP) or as part of your COOP/COG Plan.

The MYSPMP/or multi-year strategy section of your plan, should address short and long term COOP/COG goals, objectives, timelines, budgetary requirements, planning and preparedness considerations, and planning milestones or tracking systems to monitor accomplishments. It should include a prioritized list of vulnerabilities that have been identified for your organization. If the organization opts to create a separate MYSPMP, it should be referenced in the COOP/COG Plan.

A. COOP/COG PLAN MAINTENANCE

This section should address how the organization plans to ensure that the COOP/COG Plan contains the most current information. It should describe the organization's maintenance strategy and tactics, including event-driven changes and periodic reviews. Organizations should review the entire COOP/COG Plan at least annually. Key evacuation routes, roster and telephone information, as well as maps and room/building designations of alternate locations, should be updated as changes occur.

ANNEXES

Annexes contain highly detailed and necessary information, typically as either backup or reference material. Some annexes may include information typically contained in appendices. Other annexes may contain information or references to material that are owned and housed by departments, division, branches, or sections outside the COOP/COG plan itself. The annexes listed in this template contain the minimum information that should be included in a COOP/COG plan. You should include any additional annexes required for your organization's COOP/COG Plan. No particular order or sequence is required for Annex material.

Annex A: Authorities and References

This annex should cite a list of authorities and references that mandate the development of this COOP/COG Plan, and provide guidance towards acquiring the requisite information contained in this COOP/COG Plan.

Annex B: Operational Checklists

This section should contain operational checklists for use during a COOP/COG event. A checklist is a simple tool that ensures all required tasks are accomplished so that

the organization can continue operations at an alternate location. Checklists may be designed to list the responsibilities of a specific position or the steps required to complete a specific task. Sample operational checklists may include:

- ❑ Telephone Cascade
- ❑ Emergency Calling Directory
- ❑ Key Personnel Roster and Essential Functions Checklist
- ❑ Senior Activation Team (SAT) Roster
- ❑ Emergency Relocation Team Checklist
- ❑ Alternate Site Checklist
- ❑ Emergency Operating Records and IT Checklist
- ❑ Emergency Equipment Checklist

Annex C: Essential Functions

This annex should include a list of your identified essential functions.

Annex D: Alternate Location/Facility Information

This annex should include general information about the alternate location/facility. Examples include the address, points of contact, and available resources at the alternate location.

Annex E: Maps and Evacuation Routes

This annex should provide maps, driving directions, and available modes of transportation from the primary facility to the alternate location. Evacuation routes from the primary facility should also be included.

Annex F: Definitions and Acronyms

This annex should contain a list of key words, phrases, and acronyms used throughout the COOP/COG Plan and within the COOP/COG community. Each key word, phrase and acronym should be clearly defined.

Annex G: Concept of Operations

This annex should contain the operational details and procedures necessary to execute the provisions of the plan. This is a short document that includes activation procedures, notification, team membership, responsibilities, and sample task lists.