DON CMPG 2.0

Department of the Navy Critical Infrastructure Protection Consequence Management Planning Guide

SECOND EDITION

DEPARTMENT OF THE NAVY

CRITICAL INFRASTRUCTURE PROTECTION

CONSEQUENCE MANAGEMENT PLANNING GUIDE

SECOND EDITION

6 OCTOBER 2004

DEPARTMENT OF THE NAVY

CRITICAL INFRASTRUCTURE ASSURANCE OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

6 October 2004

I am pleased to provide the Second Edition of the Department of the Navy (DON) Consequence Management (CM) Planning Guide. This Second Edition offers Base Commanders and Installation Owners a valuable tool in developing plans to manage the consequences of disruptive events affecting their installations, with the key goal of maintaining the continuity of their operations, a critical aspect of building Navy and Marine Corps mission assurance.

This Guide supersedes the First Edition, and provides significantly more information on how to develop, write, and implement a CM plan. This edition better assists planners in identifying the Mission Essential Functions that define their Installation's critical contributions to the DON warfighting effort, and that are the focus of CM planning. This latest edition offers a 10-step process for developing and writing a CM Plan that can be used by installations of any size or activity, and includes measures to implement CM plans so as to ensure their continuing effectiveness. Examples of implementing measures and tools are included in the expanded list of Appendices, as well as an expanded reference list to provide depth to individual CM programs.

The information, procedures, and considerations included in the Second Edition are the result of feedback from users of the First Edition of this Guide, and are based on observations and lessons learned through the Naval Integrated Vulnerability Assessment process within the DON's Critical Infrastructure Protection program. As with all CM plans resident across DON installations, this Guide is a living document that will improve based on its continuous use by planners, and feedback to the DON Critical Infrastructure Assurance Office.

Mission Assurance rests upon the continuous efforts to maintain essential functions despite the known and unknown effects of any hazard, and requires a cooperative investment of time, energy, and resources throughout the Chain of Command. I urge each of you to use this Guide in support of your CM planning, and encourage feedback concerning its implementation.

D.M. Wennergren

CONTENTS

Foreword.....v
Executive Summary.....ix
Part I - Introduction.....3
CIP Background
CIP Event Cycle
CIP Interrelationships
The Purpose of Consequence Management Plans
Terminology
Three Dimensional Planning
Part II - Developing Consequence Management Plans.....17
Step 1 - Establish and Orient the Planning Team
Step 2 - Propose MEFs
Step 3 - Assemble Information and Analysis
Step 4 - Leadership Approval of MEFs
Step 5 - Identify CM Actions
Step 6 - Estimates of Supportability
Step 7 - Write the Plan
Step 8 - Plan Approval
Step 9 - Distribute the Plan
Step 10 - Implement the Plan
Part III - Implementation.....31
Implementation Plan
Consequence Management Exercises
National Incident Management System
Appendix A - Commanders CIP-CM Planning Worksheet.....39
Appendix B - Risk Assessment & Analysis Tools.....51
Appendix C - CM Plan Characteristics.....63
Appendix D - Planning Considerations.....81
Appendix E - CM Plan Format.....129
Appendix F - Exercises.....155
Appendix G - Abbreviations and Acronyms.....169
Appendix H - Terms and Definitions.....173
Appendix I - Consequence Management Reading and Reference List.....183

FOREWORD

This Second Edition of the Department of the Navy (DON) Critical Infrastructure Protection (CIP) Consequence Management (CM) Planning Guide provides a methodology to assist DON CIP CM planners at all Department installations, regardless of size/scope, to develop approaches that will maintain continuous operation of mission essential functions (MEFs) throughout disruptive incidents.

The goal of the CM Planning Guide is to:

- Maximize warfighting capability by maintaining MEFs throughout the life of a disruptive event,

  and

- Establish the foundation for long-term reconstitution.

This guide supports SECNAVINST 3501.1, which established the DON CIP Program. The focus of DON CIP is to provide warfighter mission assurance. SECNAVINST 3501.1 mandates participation by all hands to identify possible vulnerabilities, protect MEFs from disruption, and if disrupted by events, minimize the impact on the mission. Such events might be a terrorist attack or other act of war, an accident, or a natural disaster.

This guide is provided by the DON CIAO to give Navy/Marine Corps installation commanders direction for developing effective CM plans. It also identifies and addresses all actions, direct and indirect, that maintain an organization's continuity of operations while limiting degradation. Navy and Marine Corps activities, installations, commands or units should use this document to develop their own individual CM Plans. Each plan should address a wide spectrum of disaster events, be customized to reflect the particular requirements of their MEFs, and incorporate any existing disaster response and recovery plans as appropriate. Assistance in understanding this guide and the CM processes described herein may be obtained by contacting the DON CIAO staff at: 703.602.4412.

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Continuity of Operations is defined as "the capability of a DOD Component to continue mission-essential functions without unacceptable interruption" (DOD Directive 3020.26 of May 26, 1995 (Continuity of Operations (COOP) Policy and Planning)). How an activity manages the consequences of a disruptive event directly impacts its ability to maintain operations. Therefore, Consequence Management is the technique used to maintain Continuity of Operations.

Interdependencies affecting operational capabilities and the business processes supporting those capabilities complicate the practice of CM planning. The private sector contributes over 85 percent of the Nation's critical infrastructure, which means that - to maintain mission essential functions (MEFs) - DON entities most likely rely on resources and support services that are outside their control. This dependency on outside resources requires a more rigorous and detailed approach to determining an organization's MEFs and the elements that support and sustain them. Such interdependencies also make imperative the development of a comprehensive, multi-dimensional CM plan that covers all possible angles of MEF continuity. That need was a key driver in the development of these CM Planning Guides.

This Guide provides a methodology to develop task-oriented CM plans that integrate the dimensions of Function (organizational entities such as IT/IS, Utilities, Legal, etc), Time (the four phases of a disruptive event), and Ownership (internal/external). This three-dimensional approach enables Continuity of Operations by maintaining an organization's MEFs with minimal interruption or degradation during a disruptive event.

The Four Event Phases that Consequence Management Plans follow are:

1. Pre-Event Phase: involves organizing, planning, equipping, testing, training, and exercising actions aimed at maintaining the operation of mission essential functions without interruption or degradation of service;

2. Response Phase: focuses on the immediate reaction and response to an event;

3. Recovery Phase: involves actions to recover and restore operational capabilities (physical, cyber, or process) of mission essential functions;

4. Reconstitution Phase: includes activities to restore an asset to its pre-event design and function and/or incorporates improvements that increase functionality and survivability.

This Guide enables any Navy/Marine Corps activity to produce a fully integrated CM Plan. It first provides the reader with a brief overview of terminology and relationships that are beneficial to understanding the approaches discussed later in the document. A summary of Secretary of the Navy CIP policy guidance and DON CIP background is provided to explain the rationale and impetus behind the Department's CIP Program.

Each component of a CM plan is addressed, providing guidance on content as well as additional considerations necessary to achieve integrated plans based on the fifteen functional areas of CM that typically support each DON organization. This discussion enables CM planners to understand the relationships between various decision options as well as improve the operational results of those decisions. Appendices provide information on topics such as Conducting a Vulnerability Assessment, Decision Analysis, CM Plan Assessment, and a Sample Scenario with Analysis. Where specific document sources are not identified, standards for planning are based on an analysis of findings and lessons learned from vulnerability assessments, disaster after-action reports, and a variety of government and private sector best practices.

In summary, this Second Edition builds on the foundation established in the first publication and reflects feedback from the DON community (a Summary of Changes page follows). By providing a comprehensive instructional guide for effective CM Plan development, a clear, concise roadmap exists to achieve the primary goal of the DON CIP Program providing mission assurance for our warfighters.

SUMMARY OF CHANGES

SINCE THE FIRST EDITION

Summary of Changes
Since the First Edition

Based on input received from field activities and the continuing research and analysis of emerging trends, the changes incorporated into this Second Edition include:

- Expanding the level of detail describing how to develop and write a plan.
- Adding an example of how the issues considered during the planning cycle actually appear in a final plan.
- Providing more definitive procedures to determine MEFs with more clarity.
- More detailed guidance on planning, conducting, and learning from exercises.
- A checklist of characteristics found in successful well-written plans.
- Points of contact for assistance.
- Expanding the 12 Functional Areas found in the First Edition to 15 by adding, Legal, Command and Control, and First Responders.
- A bibliography containing reference material about consequence management planning.
- Expanded tenant-host planning considerations to better understand issues from both perspectives.

PART I:
INTRODUCTION

PART I: INTRODUCTION

1. TERMINOLOGY

Understanding two terms - Mission Essential Functions and Critical Infrastructure - is essential in the development of meaningful CM Plans.

- **Mission Essential Functions (MEFs):**

SECNAVINST 3501.1 of 16 June 2002 defines "Mission Essential" as any function that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. MEFs are those specific functions required to perform the primary mission of a DON asset. Such functions are limited to actual processes, and do not include supporting processes. For example: if the DON asset is a communications station, it might be determined that the MEFs are how it receives, processes, and transmits classified messages. The operation of housing, dining facilities, fuel stations, etc., **though obviously important to the installation population, may not directly generate the strategic value of the installation** and so would not be identified as MEFs (see Figure I-1). Appendix A provides a detailed methodology to review organizational missions and determine specific MEFs enabling those missions. The process also identifies the functional areas on which the MEFs primarily depend, as well as the critical assets required to perform the functions, and internal and external dependencies on which the MEFs rely.

FIGURE I-1. MEFS = FUNCTIONS REQUIRED TO GENERATE THE STRATEGIC VALUE OF A DON ENTITY.

The scope of MEFs may be more extensive during contingencies or wartime than they are in a peacetime environment and planners should develop their CM plans accordingly. Planners should also take into account the fact that MEFs, and therefore the assets that house them, may be physically separated on an installation. For example, a communications site might have its antennae located on a remote hill and its receivers and transmitters located in an industrial complex. Utilities supporting the communications site might be located in a third area on the installation and the administrative processing and storage activities may be housed in a fourth location. Taken together, these locations provide the physical characteristics of the MEFs that reside on this installation. MEFs are the responsibility of a specific command or unit and consist of the processes used to develop deliverables and the deliverables themselves.

- **Critical Infrastructure:**

Critical infrastructure consists of those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations. Loss or degradation of these assets jeopardizes the ability of the Department of Defense to execute the National Military Strategy. Within the context of CM planning, an asset may be any entity such as installation, command, unit, system, equipment, etc. (described in Appendix H Terms and Definitions) depending on the MEF supported and the breadth of the Command.

The value of each critical asset is generated through its MEFs, which provide strategic utility to the DON and Combatant Commanders. Loss of a critical asset may involve the physical destruction of the asset, or the loss or degradation of the asset's MEFs. It is important to realize that critical assets may be totally dependent upon DON infrastructure, totally dependent on commercial infrastructure, or a combination of both. The ever-increasing interdependencies have also increased the threat to critical assets. CM planners must have a clear understanding of the interdependencies of their critical assets before they can successfully construct CM plans for their protection.

2. CIP BACKGROUND

In a 26 August 1999 memorandum, the Under Secretary of the Navy appointed the DON Chief Information Officer (CIO) as the DON Critical Infrastructure Assurance Officer (CIAO) "...in order to provide a comprehensive approach to protecting the Department's critical infrastructures." On 16 June 2002, the Secretary of the Navy signed SECNAVINST 3501.1 (http://neds. nebt.daps.mil/directives/3501_1.pdf) to formalize the DON Critical Infrastructure Protection (CIP) Program and directly relate the DON CIP Council and the DON CIP Working Group to the Department of Defense (DOD) CIP organization. In executing the policies contained in SECNAVINST 3501.1, the DON is in concert with the requirements of the National Plan for Information Systems Protection, Homeland Security Presidential Directive # 7, the DOD Critical Infrastructure Protection Plan and the Defense-wide Information Assurance Program.

The focus of the DON CIP Program is to provide warfighter mission assurance. CIP encompasses traditional aspects of security: Anti-Terrorism/Force Protection, Operational Security, Physical Security, and Information and Infrastructure Assurance. A key aspect of CIP is recognizing the importance of DON Critical Assets (CA) in supporting Regional Combatant Commander requirements, particularly Combatant Commander Operations Plans (OPLANs), thus it is also considered a critical element in acquisition and operations planning that supports overall mission assurance by linking assets to DON operations.

3. CIP EVENT CYCLE

The six phases of the CIP cycle span activities occurring before, during, and after events – which could be hostile acts, accidents, or natural disasters - that may result in infrastructure destruction or disruption (Figure I-2).

The CIP event cycle involves two modules:

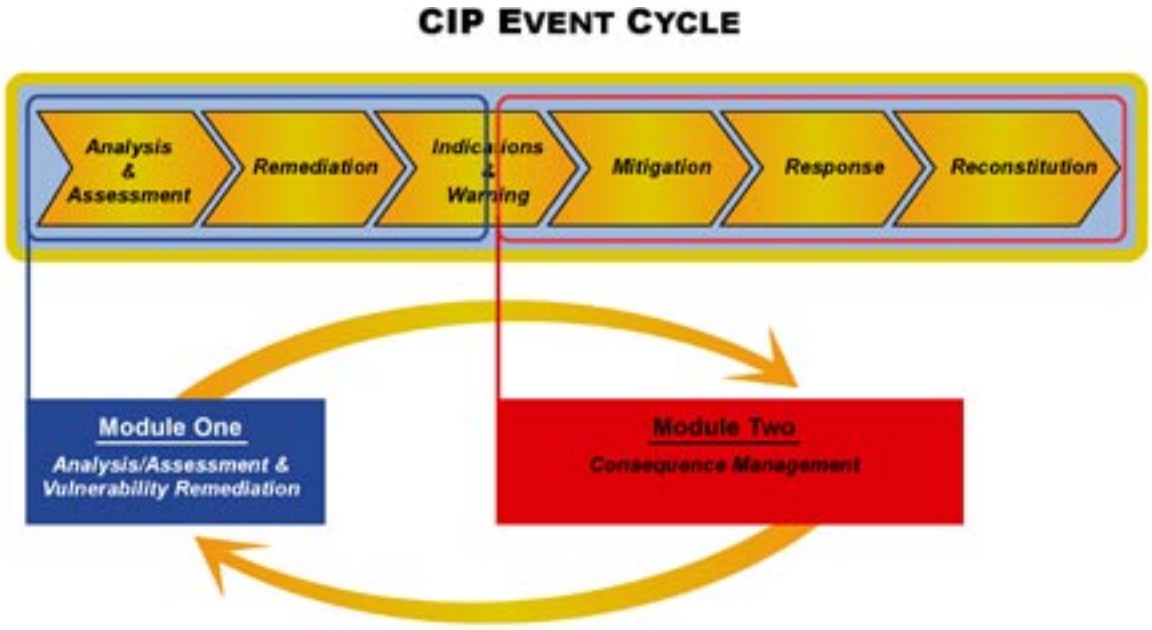


FIGURE I-2. THE CIP EVENT CYCLE INVOLVES SIX PHASES: INFRASTRUCTURE ANALYSIS AND ASSESSMENT, REMEDIATION, INDICATIONS AND WARNING, MITIGATION, RESPONSE, AND RECONSTITUTION

The first module represents the activities that take place prior to an event in order to prevent occurrence or minimize impact. The second module represents the pre-planned actions that take place in response to an event.

4. CIP INTERRELATIONSHIPS

The strength of DON CIP CM is the integration of the Pre-Event Plan with the supporting Response, Recovery, and Reconstitution Plans. Integrating these plans provides critical asset owners with a documented, event centered process enabling timely restoration of critical functions should a disruptive event occur.

An important issue to understand when writing a CM plan is the relationship and interdependency of the "during and after the event" execution of CM Plans to the organization's Critical Infrastructure Protection program. These relationships and interdependencies are depicted in Figure I-3.

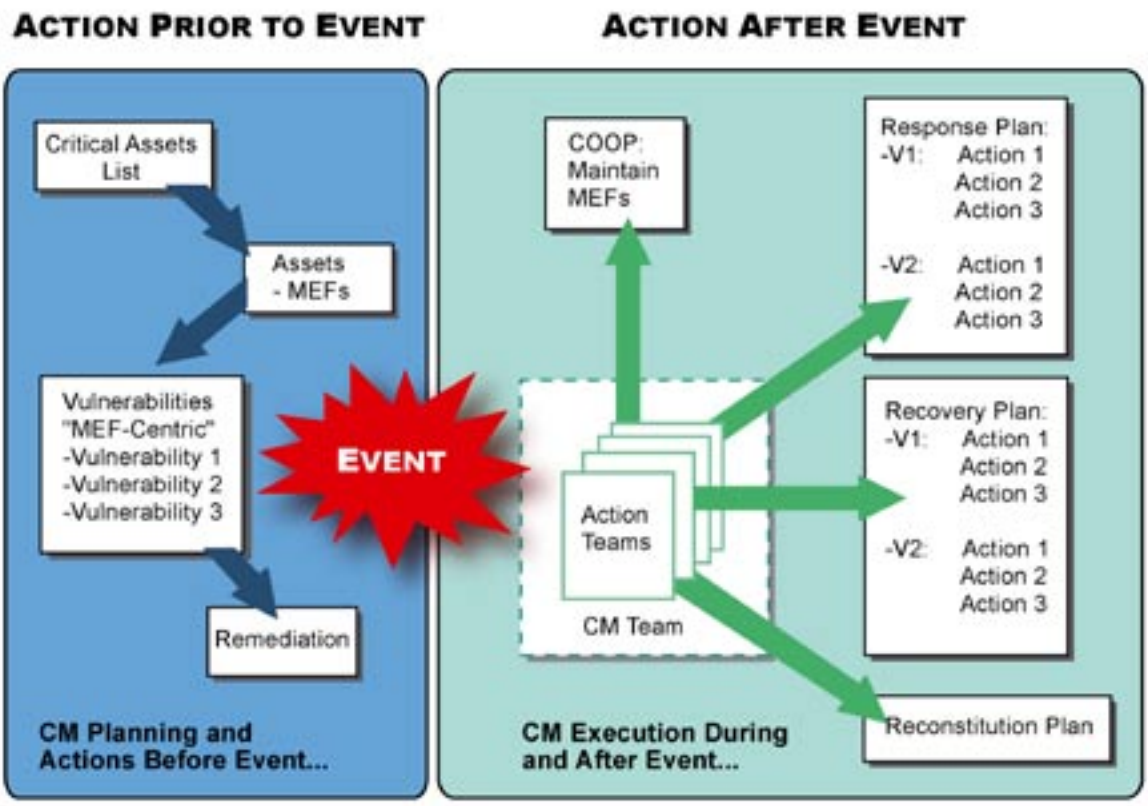


FIGURE I-3. INTERRELATIONSHIPS BETWEEN THE CIP CYCLE AND CONSEQUENCE MANAGEMENT

5. THE PURPOSE OF CONSEQUENCE MANAGEMENT PLANS

Continuity - Consequence Management Interrelationships

CM planning focuses on minimizing the disruptive effects of an event on an organization's Mission Essential Functions (MEFs), and on planning for the maintenance, recovery and restoration of these functions.

CM planning thus supports continuity of operations in an all-hazards environment. The CM planner identifies actions required to maintain and recover each MEF based on the particular vulnerabilities affecting the MEFs. Upon execution CM plans enable organizations to:

- Develop and maintain situational awareness of the event and its impact
- Adapt its plans in order to:
  - Manage and control the event; while maintaining command and control of the organization in order to continue the mission.

The strength of CM planning is the holistic approach to integrating the actions taken during the various phases of an event. Integrating the actions during these phases provides commanders with a documented event-centered process enabling timely restoration of MEFs should a disruptive event occur. Figure I-4 shows how the CM planning process exists before, during, and after a disruptive event. Before an event occurs, organizations analyze vulnerabilities and risks; write plans to maintain operational continuity; make the policy, investments, agreements, etc., necessary to implement the plan; and build their ability to execute the plan through tests, training, and exercises. This cycle continues until an event occurs.

During an event, organizations maintain operational continuity by responding to the disruption, recovering capability, and reconstituting as required. After the event, organizations transition back to a "pre-event" posture while analyzing lessons learned to generate improvements to their plan.

Before addressing the construction of the CM plans, it is important to discuss several key terms, elements, and background relevant to the DON CIP CM Planning process.

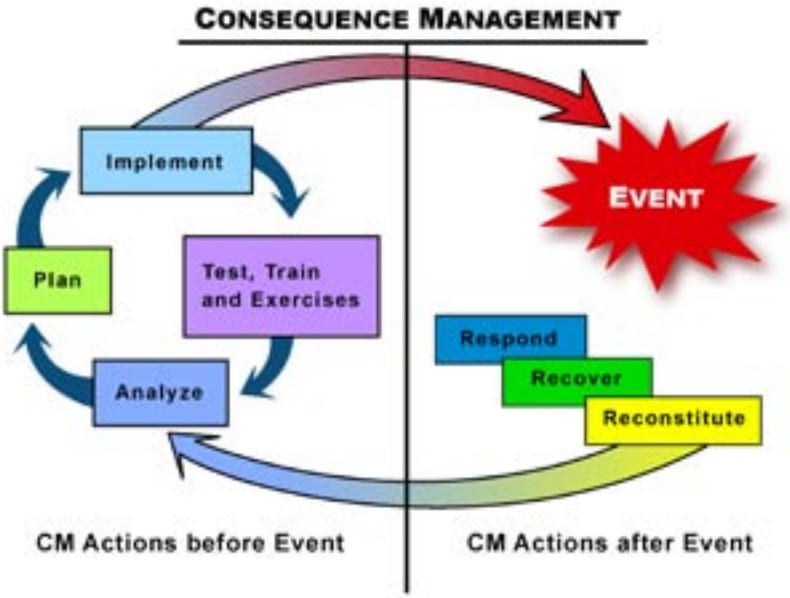


FIGURE I-4. CONSEQUENCE MANAGEMENT PLANNING CYCLE

6. THREE DIMENSIONAL PLANNING

Figure I-5 depicts the 3-dimensional approach to CM planning used within the DON. The three dimensions are functional areas, event phases and ownership or control.

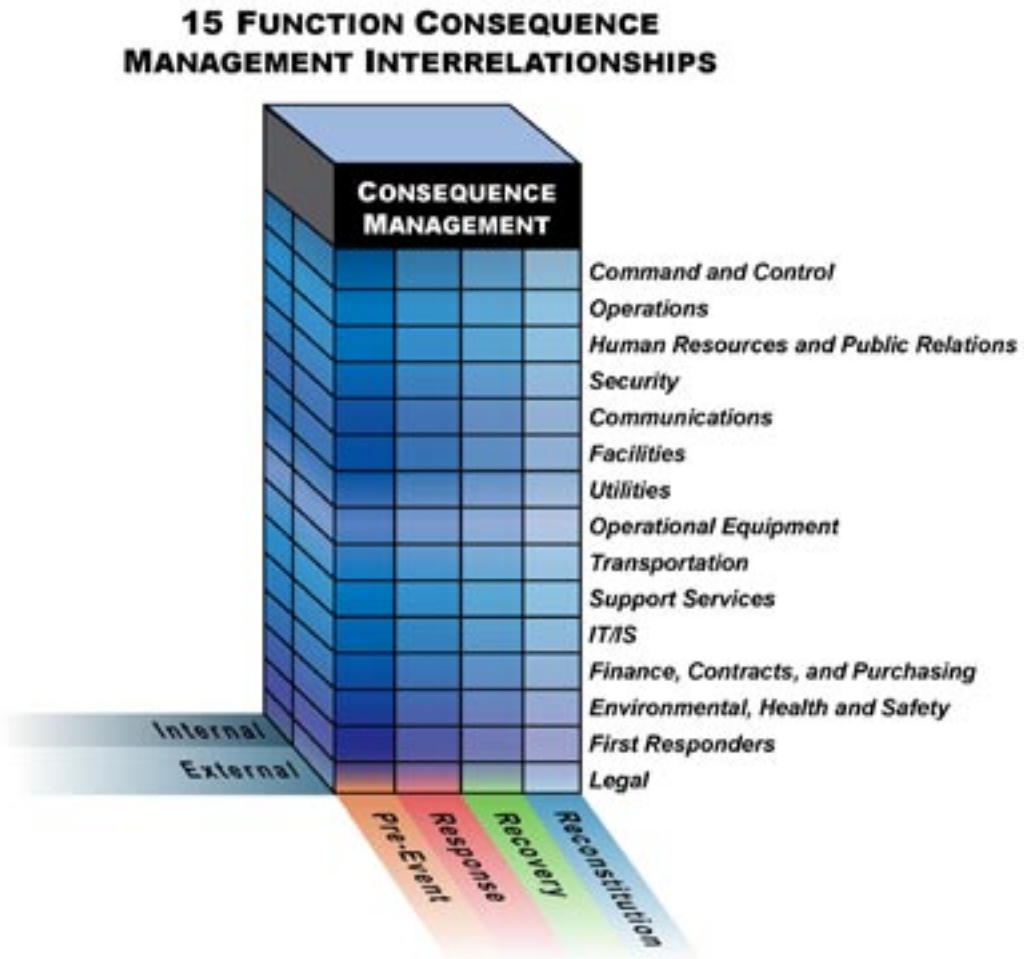


FIGURE I-5. CONSEQUENCE MANAGEMENT PLANNING MODEL

THE FIRST DIMENSION CONTAINS THE 15 FUNCTIONAL AREAS:

1. **COMMAND AND CONTROL** includes the people and procedures necessary to sustain leadership's ability to maintain situational awareness of on-going events while exercising leadership decision making processes, etc.

2. **OPERATIONS** include mission requirements, MEF sustainment, operational requirements, shared services, MOUs, MOAs, and inter/intra relationships of decisions made in other functional areas.

3. **HUMAN RESOURCES AND PUBLIC RELATIONS** include recall, points of contact, alternate Human Resources sourcing, training, Freedom of Information Act (FOIA) issues, recruiting, identification, skill sets, and Media Relations, etc.

4. **SECURITY** includes physical and cyber security, security clearances, safeguarding classified or proprietary documents and equipment, surveillance and intrusion detection equipment, escorts, traffic control and routing, Chemical Biological Nuclear Radiological and Explosive (CBNRE) detection equipment, and coordination with local, State, or Federal security and law enforcement officials, etc.

5. **COMMUNICATIONS** include mass notification systems, all telecommunications (landline and por table), mobile radio, and facsimile transmissions, etc.

6. **FACILITIES** include physical structures, identification of alternate facilities, parking, health and comfort requirements, office furniture, etc.

7. **UTILITIES** include electrical power, water, Heating Ventilation and Air Conditioning (HVAC), fuel, utility sourcing, alternate providers, etc.

8. **OPERATIONAL EQUIPMENT** includes engineer, transportation, WMD detection, HAZMAT and WMD response, etc.

9. **TRANSPORTATION** includes passenger, cargo, heavy equipment transporters, traffic flow, and interac tion with local, state, or Federal movement control agencies, etc.

10. **SUPPORT SERVICES** include contracted services, service provider organizations, and alternate sources of services, and possible outsourcing for lost or diminished capabilities, etc.

11. **INFORMATION TECHNOLOGY/INFORMATION SYSTEMS (IT/IS)** includes all aspects of IT/IS support and processing capabilities to include communication, networking, data manage ment, analysis, operating systems, applications, peripherals, system certification, hardware, software, IT maintenance and services, etc.

12. **FISCAL, CONTRACTING, AND PURCHASING** includes funding estimates for incident response and recovery preparation that impacts the MEF, to include the processes to request, authorize and expend funds in support of the MEF.

13. **ENVIRONMENTAL, HEALTH AND SAFETY** includes all medical services, Occupational Safety and Health Administration (OSHA) compliance requirements, infrastructure, Human Resources and capabilities supporting the MEF.

14. **FIRST RESPONDERS** includes local fire and rescue, hazardous material response, law enforcement, and mechanisms and procedures to tap into State and Federal responders.

15. **LEGAL** includes insurance, liability, governance, labor relations, contract issues, regulatory compliance, etc.

The second dimension contains the four phases of a disruptive event, against which organizations must focus their efforts. The following discussions detail each in terms of their makeup and integration into other internal and external characteristics of the CM plan.

THE SECOND DIMENSION CONTAINS THE EVENT PHASES:

THE PRE-EVENT PHASE - the most important phase - addresses all actions, procedures, and policies necessary during the period before a disaster or interruption occurs, and thus lays the foundations for continuity of operations. This timeframe leading up to a potential interruption of 'business as usual' is the planner's opportunity to integrate the various elements of integrated CM into the organizations' operational methods, as well as any business process reengineering to remediate risk. During the Pre-Event Phase, organizations analyze and assess their vulnerabilities; write, test, train and exercise their plans; and invest in assets and partnerships to strengthen their ability to withstand a disruption. Figures I-3 and I-4 depict this phase.

THE RESPONSE PHASE focuses on the reaction and response to the disaster event regardless of its origin, be it criminal action, accident or natural disaster. The Response Phase should contain steps to notify, activate and mobilize the response team and external service providers to maintain business operations, and to limit damage or disruption caused by the event. The external service providers may include local community leaders, medical services, hospital hazmat, and law enforcement agencies. The Response Phase should also address requirements for expertise from all working and engineering levels of the business unit at the facility, infrastructure and function level.

THE RECOVERY PHASE reestablishes critical functions that sustain the organization through recovery and restoration of physical and cyber infrastructure and processes. Typically, one expresses interruption or degradation of MEFs in terms of time increments relative to the loss of function. The Recovery Phase should contain steps to notify, activate and mobilize the recovery team and external service providers to recover and restore critical infrastructure functionality. Note that each MEF may have separate time-related impacts and recovery actions that are different from other recovery actions. The Recovery Phase may entail effecting repairs, bringing in internal or external expertise (public or contracted) or activation of backup infrastructure or facilities.

THE RECONSTITUTION PHASE seeks to restore the critical infrastructure and functions to their original pre-disaster event design and function, or incorporate new technology, processes, construction techniques, etc. to improve the functionality and survivability of the critical infrastructure and its MEFs. For example, a satellite node that provides enhanced functionality and security might replace a traditional telecom node.
An analysis of each identified MEF across the CM Phases identifies the specific issues associated with its maintenance, restoration, or reconstitution.

THE THIRD DIMENSION CONTAINS OWNERSHIP OR CONTROL:

The third dimension, internal or external ownership, often dictates the nature of how the capability integrates into the plan. When dealing with internal assets and capabilities, planners must fully understand internal policies and procedures necessary to employ the asset or capability. When dealing with external agencies, planners must first understand the agency's procedures, organization, and command and control systems in order to effectively plan for support. In either instance, planners should clearly identify their requirements and gain an understanding of the capabilities and limitations of the assets and capabilities in order to deconflict any planning issues, and develop their CM plan accordingly.

HOST/TENANT ISSUES

Many DON activities are tenants aboard a naval or other service host installation. In these instances, the host installation is responsible to provide common base support services including public works, logistics, maintenance, security, etc. Planners should involve the host in the planning process to identify and resolve any gaps between the planner's requirements and the host's ability to provide support. During this process it is important to establish the priority of support that the tenant planner may expect from the host installation. In those instances where the planner is a member of the host installation staff, the planner should make it a point to be involved in the CM planning of each tenant to ensure the host command is aware of and supports their specific requirements, has deconflicted the use of space and resources aboard the installation, and developed the priority of effort to support the tenants.

This three dimensional approach allows a planner to place things into perspective, based upon the organization's goals and the identified MEFs, and will assist in the systematic integration of a CM plan as the process unfolds. When planners begin to analyze MEFs across the phases, time may invalidate some MEFs. For example, although it may be critical to restore utilities capabilities in order to restore a base installation's sustained force deployment capability, it may be some time before disruption of that capability by an event affects short-term deployment timelines in a crisis. The planner can further take steps to remediate potential negative outcomes during the Pre-Event Phase through development of redundant capabilities.

MANAGEMENT OF CM WITHIN THE ORGANIZATION

There are several ways to incorporate and manage CM within a DON organization, and arguably no single right way. Any organization must examine its mission and organization, and develop a CM management process that fits their circumstance. What follows are some command, organizational, and facilities considerations for the CM Planner to use in developing an approach to CM.

Consequence Management typically requires centralized coordinated planning with decentralized execution. While senior leadership maintains strategic control of the organization, they cannot make every decision, and must provide the means for on-scene decisions with informational update reports. Additionally, since the Response, Recovery, and in some cases, Reconstitution may happen concurrently, leadership must integrate these efforts while maintaining current operations, and future operations planning.

One method of implementing and coordinating these concurrent activities is to organize, train, and employ a series of CM Teams to manage each phase of the event. Composition of the teams depends on the size, physical dispersion, and complexity of the organization. These teams generally include the Response Team, the Recovery Team, and the Reconstitution Team. Figure I-6 depicts a notional CM Team organization. The CM Team exercises overall management and oversight for the entire CM program, including Pre-Event

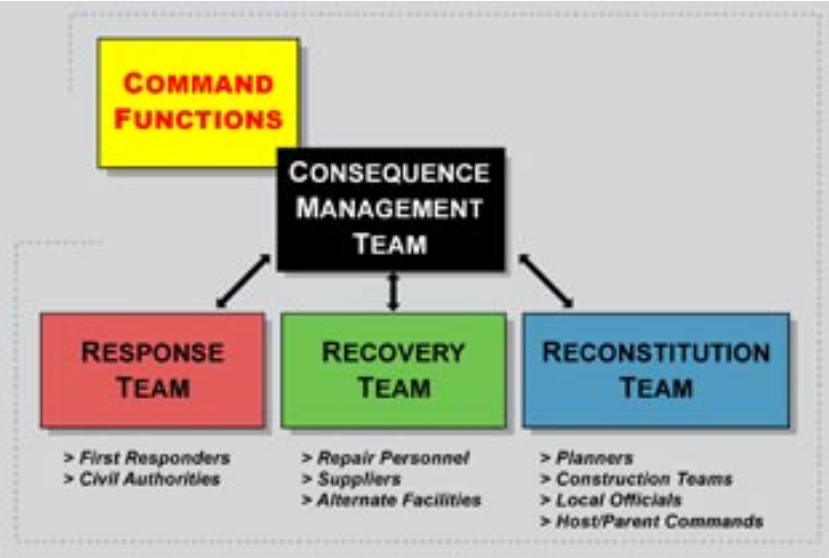


FIGURE I-6 NOTIONAL CM TEAM ORGANIZATION

training and education, equipping the CM Teams and the organization itself in preparation for executing the CM Plan, and conducting exercises and inspections. When executing the CM Plan, the CM Team operates the organizations' Emergency Operations Center to focus on management of the event while allowing the unit to remain focused on operations. The CM Team exercises control of the event through the employment of three sub-teams, described as follows.

The Response Team focuses on the initial reaction to the event. It assesses the nature and extent of the disruption, ensures accountability of all people, and assists First Responders in their efforts.

The Recovery Team focuses on how the organization will regain immediate and mid-range operational capability. Members of the Recovery Team include maintainers and operators sufficient to provide the nucleus of the recovery effort and, augmented based on the Response Team's damage assessment, initiates actions to restore MEF functionality. The Recovery Team is trained to receive information from the Response Team, assess any damage or operational limitations and effectively activate and direct the effort to recover operations.
The Recovery Team also provides critical information to the Emergency Operations Center that supports leadership's efforts to fully recover operations and prepare for the Reconstitution phase. Note that the Recovery Team integrates its efforts toward recovery with those of the other teams in each of the phases including internal and external support providers. The quick decisive actions of the Recovery Team enable the organization to maintain its MEFs throughout the disruptive event.

The Reconstitution Team takes the long-range view of the event and focuses on how the organization might regenerate or replace lost capabilities. Its purpose is to provide senior leadership with the information they need to decide whether to reconstitute the "as-is" or forge a new "will be" capability. The team must maintain situational awareness of the current requirements of the organization, but also of emerging technologies and practices that might better enable the business to operate in the future.

Facility requirements for each CM team are a function of the CM Plan and the MEFs to be protected. The CM Team may, but is not required to be, co-located in the same facility as the operations staff. The CM Team's location should allow them to best inform and advise the command while remaining distant enough to reduce mutual interference with either operation. The long-range, post event nature of the Reconstitution team may facilitate their working out of the headquarters location, while the Response and Recovery teams' activity requires a highly mobile effort. Refer to Appendix D - Planning Considerations for more detailed facility issues.

PART II:
DEVELOPING CONSEQUENCE MANAGEMENT PLANS

Part II: Developing Consequence Management Plans

INTRODUCTION

Planning is the act of envisioning, determining, and documenting effective ways of achieving a desired objective or end-state. Through the process of developing plans, then maintaining and exercising those plans, an organization:

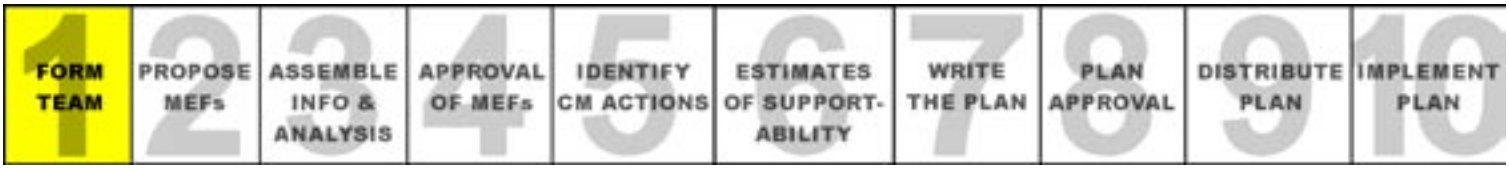
- Identifies actions required in response to anticipated events, along with those individuals responsible for their implementation.
- Develops a shared awareness of situations planned or anticipated among members of the organization, thereby enabling and encouraging informed initiative at all levels.
- Generates expectations within the organization of how events will unfold and the response to those events. This empowers members of the organization to manage events rather than simply react to them.

A few basic tenets of the CM planning process are worth remembering for both seasoned planners and those just starting out:

- The process of generating a CM plan may in part dictate its success or failure. If done well, the planner can expect to achieve the aims described above. If accomplished in an information vacuum or without coordination, the plans will likely not achieve their purpose.
- Planning supports decision-making. As such, planning is a top-down process, empowered by organi zational leadership committed to - and part of - the planning effort. Without a charter, a planning team can quickly find itself at cross-purposes.
- Integrated planning requires a disciplined approach to ensure coordination and thoroughness. The 10-step planning methodology described herein is applicable to operating forces as well as supporting shore establishments, and supports organizations of any size. The focus of this discussion is on the ten steps required to write the plan. Successful planning will require essential information to answer the following three questions:

- Where is the organization vulnerable?
- How will a disruption affect the organization?
- What are the current risks to the organization?

The process to build a CM Plan is weighted towards the first 5 steps. Experience indicates that as much as 80% of the planning effort should be concentrated here.



STEP 1. ESTABLISH AND ORIENT THE PLANNING TEAM.

Building a CM plan requires an organizational commitment at three basic levels.

- Executive leadership must provide the guidance, support, and authority necessary to sustain the effort and ensure buy-in across the organization.
- Operational management provides the functional level oversight and 'bigger picture' perspective to guide the outcomes of the plans.
- Working level subject matter experts provide the detailed understanding of organizational core processes.

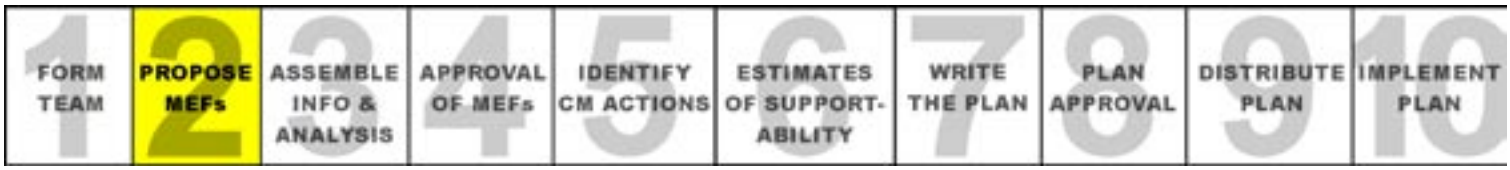
Teamwork is essential. Planners should not overlook the contribution of teamwork even in cases where circumstances (such as a small, single facet organization) may tempt the CM planner to go it alone. Whether a single team develops the entire plan, or a planning team produces each phase of the plan is a function of the organizations' size, complexity, and leadership prerogative.

The Benefits of Using a Team Approach

Several factors drive the team concept to CM planning. Among them are the synergy of group dynamics, collective time and energy advantages, and the broad perspectives of subject matter experts. Most importantly, however, the planning team itself is part of the process, which ultimately will integrate CM planning into the entire organizational process; into the daily cycle of the organization. By including key representatives from the unit functional areas, the planner:

- Builds consensus, or buy-in, as part of the plan development.
- Develops feedback and receives feasibility analysis as planning unfolds, rather than obtaining feedback only after a draft plan is completed.

- Ensures that each MEF is represented by one or more stakeholders; and,
- Establishes a pool of personnel who are cognizant of CM program requirements, from which to potentially draw key members of response teams.



STEP 2. PROPOSE MISSION ESSENTIAL FUNCTIONS.

This is the most important task in building a CM plan. It requires stringent objective analysis of the processes that drive the organization, as well as subjective consideration of intangibles affecting the ability of the organization to perform its mission. This step may be a validation of previously identified MEFs in organizations with existing CM plans, or in cases where MEFs have been identified within the Analysis and Assessment phase of the CIP Cycle.

Through the MEF identification process the planner conducts a mission analysis to determine the enabling functions supporting each of the organization's mission(s). Each identified function is examined to determine its importance to the mission, and draw a distinction between functions that are "essential", and those that are important yet will not necessarily impede the mission if disrupted. This will often require very subjective analysis, relying on the experience and subject matter expertise of the planning team. As there are no recognized standards to define MEFs within an organization; similar DON organizations may have vastly different MEFs. All MEFs can be viewed in terms of evaluation criteria to determine their relative importance to the command as depicted in Table II-1.

MISSION	*"Strategic" value in promoting the mission of the organization.*
SCOPE	*Generates significant value to other entities or commands.*
LOSS IMPACT	*Loss or interruption causes immediate disruptions on ability to perform tasks.*

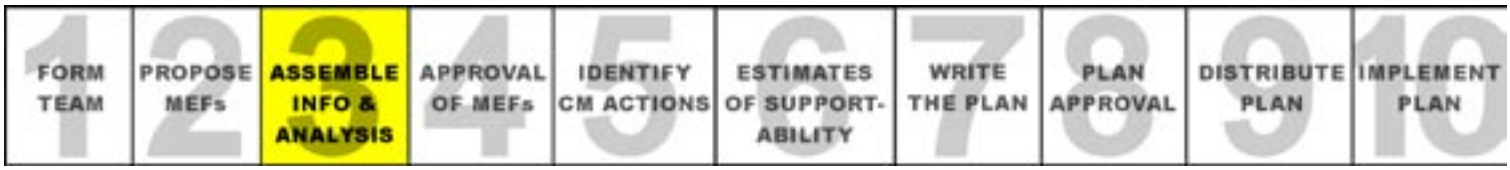
TABLE II-1

Identifying MEFs may require some organizational process analysis, but an informal exercise to help in recognizing MEFs would be to ask, "What is the mission of our unit, base, or activity?" "If we could do only one thing, what would it be?" "What gives the most value toward accomplishing our mission?" "What would the impact be if we couldn't provide this particular function or service?" The answers to these questions form the basic outline of your MEFs. Appendix A provides a detailed process to assist planners in determining MEFs , the functional areas supporting each MEF, and the critical assets required to perform the MEF.

Establishing priorities for MEFs requires a great deal of rigor and discipline. It seeks to answer, "What is the logical priority for MEFs that best assures mission success?" The prioritization process must be a joint effort by both planners

and staff, and executed for each MEF across the 4 phases. Ranking MEFs is critical to integrated planning in that doing so clearly establishes the relative importance of each MEF and identifies how the organization will preserve and recover them if disrupted. The outcome of the prioritization process is a road map for planners and staff alike to use in remediation of vulnerabilities and in writing a CM plan.

The identification of the organizations' MEFs allows the planner to look deeper into the process and identify the Critical Assets, which generate each MEF. These assets may range from cyber to physical, can be organic or from an augmentation source, internally or externally provided, or dispersed across a wide geographic area. Critical Assets also include people. The list of Critical Assets will expand and contract as validated during the planning process. In some cases, multiple MEFs may rely on a single asset such as a server or warehouse. The purpose of identifying these assets is to develop the means for protecting, restoring, or reconstituting them over the course of a disruptive event.



STEP 3. ASSEMBLE INFORMATION and ANALYSIS

This step involves the following actions:

a. Review Internal Plans and Policies. Organizational and facility level documents provide a wealth of information to augment existing plans and concepts that will contribute to the CM plan's abilities to sustain MEFs.

b. Assemble the Following Items:

- Evacuation plan
- Fire protection plan
- Safety and health program
- Environmental policies
- Security procedures
- Finance and Contracting procedures
- Organization closing policy
- Civilian employee manuals
- Hazardous materials plan
- Process safety assessment
- Risk management plan
- Capital improvement program
- Mutual aid agreements with other entities

c. Identify Applicable Federal, State and Local Regulations, Such As:

- Environmental regulations
- County or city Emergency Response Plans
- Transportation regulations
- Federal Regulations regarding disabled and non-English-speaking Human Resources
- OSHA

d. Identify Processes That Sustain Your MEFs, Including:

- Strategic products, functions and services the organization provides, and the facilities, resources, and equipment needed to support and produce them.
- Products and services provided by suppliers or external DON organizations (especially sole source vendors) upon which MEFs depend. These may not be limited to material 'things', but may include such items as utilities, transportation, or other "indirect" processes.
- External service dependencies such as electrical power, water, gas, telecommunications and transportation supporting MEF functions.
- Analyze processes and procedures for interdependencies with other internal and external assets or functions.
- Refer to Appendix A for information on developing this information.

e. Meet with Outside Groups

DON organizations rely on municipal services for a wide array of response and recovery actions, including fire and rescue, law enforcement, etc. Thus the county emergency management office (typically found in the county Fire Department) is a key player in a CM Plan. CM planners should meet with state and local government agencies, community organizations and utilities to inquire about potential emergencies and the plans and available resources for responding to them. Sources of information include:

- Mayor or County Administrator's office
- Local Federal Emergency Management Agency (FEMA) office
- Fire Department
- Police Department
- Emergency Medical Services organizations
- State and local Transportation Departments
- Public Works Department
- Local Planning Commission
- Telephone companies
- Electric utilities
- Existing business networks or organization relating to business continuity or disaster planning
- Key vendors supporting the organization

INTERNAL	EXTERNAL
Internal Communication System	*First Responders*
Emergency Management Teams	*Local Utilities Providers*
Emergency Operations Center	*FEMA*
Emergency Equipment (Mobile Electric Power)	*National Guard*
Evacuation Site	*Hospitals*
Recall Procedures	*Contractors (i.e. Maintenance, Suppliers, etc.)*

TABLE II-2. SOME EXAMPLES OF INTERNAL AND EXTERNAL EMERGENCY RESOURCES AND CAPABILITIES.

f. Identify Internal and External Emergency Resources and Capabilities

g. Conduct or assemble the results of any supporting analysis conducted to assist in prioritizing MEFs, dentifying tasks, etc. included in the CM Plan. These will include the results of Naval Integrated Vulnerability Assessments (NIVA), Business Impact Analysis (BIA), decision analysis, threat assessments, and other potential risk assessment tools.

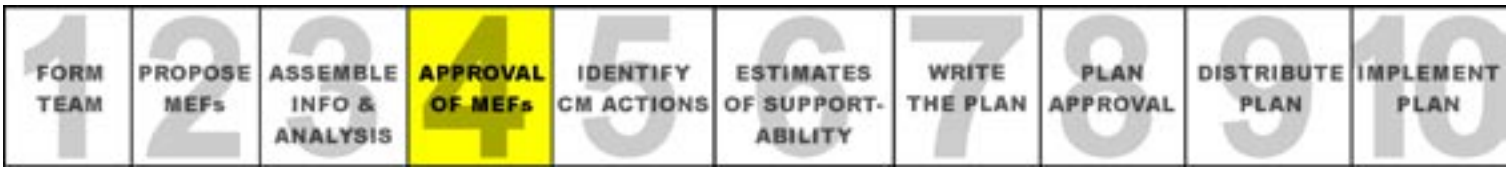
The objective of the NIVA is to:

- Identify threats to and vulnerabilities of an asset.
- Identify the associated risk to performance of essential functions.
- Take action to remediate or fix as many of the threats and vulnerabilities as possible.

A BIA may assist in determining the affects of losses of certain MEFs, and allows the application of various metrics to assist in determining recover point objectives based on selected criteria. Although normally associated with revenue-generating activities, the BIA can be useful to DON planners in determining recovery point and recovery time objectives for some MEFs.

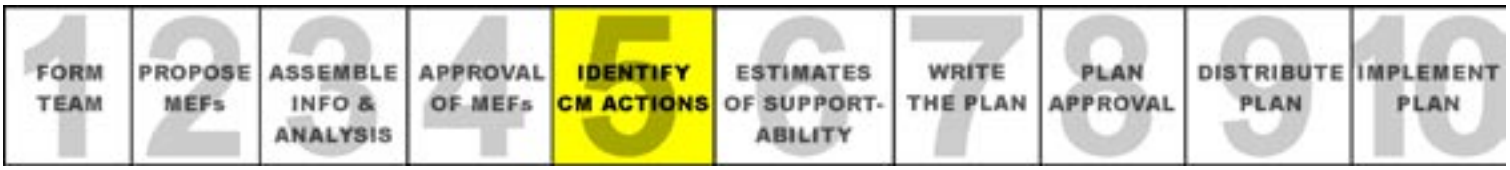
A decision analysis provides a means of applying metrics to the options available to the CM planner.

Appendix B contains a discussion of IVAs, BIAs and Decision Analysis. Threat assessments provide information on the likelihood of a disruption action occurring during a particular point in time.



STEP 4. LEADERSHIP APPROVAL OF MEFs.

This step validates the MEFs and assures the planning team does not spend time and effort in planning to restore functions that are later invalidated during the plan approval process.



STEP 5. IDENTIFY CM ACTIONS.

This step involves identifying actions to reduce the threat, mitigate the vulnerability, or restore, recover, or reconstitute each MEF identified in Step 2. This will require analyzing, deconflicting, and coordinating actions contemplated within each functional area to ensure mutual supportability within each phase, and facilitate transition between the phases. The planning team will review, compare, and consider the information collected in Step 3 with respect to each MEF in order to identify the corrective, response, recovery, and/or reconstitution actions that will form the basis for the CM Plan.

When an action within one functional area is considered, the consequences of that action must be measured within all other functional areas, through all four phases of the Plan. In a large organization this can be a lengthy, rigorous process. The planning team leader has flexibility in determining how this process will be carried out. In smaller organizations where a single team will develop and write all 4 phases of the Plan, a forum of planners may be the desirable means of developing Plan requirements. In larger organizations the team will likely choose to develop requirements by functional area, and return to the plenary session to sort out conflicts and supporting/supported relationships. In these larger sessions the use of more numerous milestones will enhance the focus and discipline of the process. In some organizations the MEFs will be easily identified, and a dominant functional area will emerge as central to the organizations' mission.

Part III of this Planning Guide presents planners with a categorized list of issues to take under consideration when developing CM requirements, and forming them into a plan. The organization of Part III by Phase and functional area demonstrates the subtle nuances that must be considered when considering actions during each phase of an event.

The planner prepares a general concept of operations, by phase, to explain how the recommended actions will be implemented and their anticipated outcomes in assuring consequence management.

Planning assumptions. Assumptions are made only in the absence of specific information concerning present or future situations. When basing CM Plan decisions on an assumption, planners should ask:

-Is it logical?

-Is it realistic?

-Is it essential for planning to continue?

-Does it avoid assuming away an insurmountable situation?

IMPLEMENTATION PLANNING

When writing a plan, CM planners must look to the future and consider the "should be" rather than limit their thinking to the "as is." This focus on the future often identifies areas in which the current organization, equipment, policies and procedures are insufficient to meet the requirements of the new CM Plan. In many instances, action is necessary to strengthen the organization against the impact of a disruption by:

- Altering processes to generate redundancies or sustain MEFs, or,
- Enacting policy to coordinate actions or events.

Therefore, the CM planner must simultaneously coordinate any necessary changes to existing policies, procedures and equipment in order to ensure they will sustain the plan when approved. Failure to coordinate these capabilities will result in a plan that speaks to the future desires of the organization, but has no practical connection to the organization's ability to execute the plan. See Figure II-1 below.

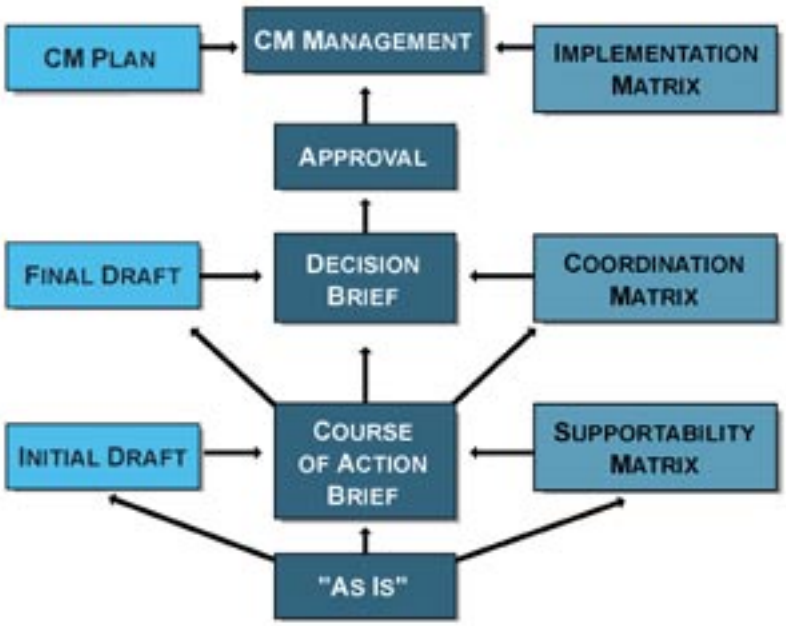


FIGURE II-1. CONCURRENT DEVELOPMENT OF CM AND CM IMPLEMENTATION PLANS

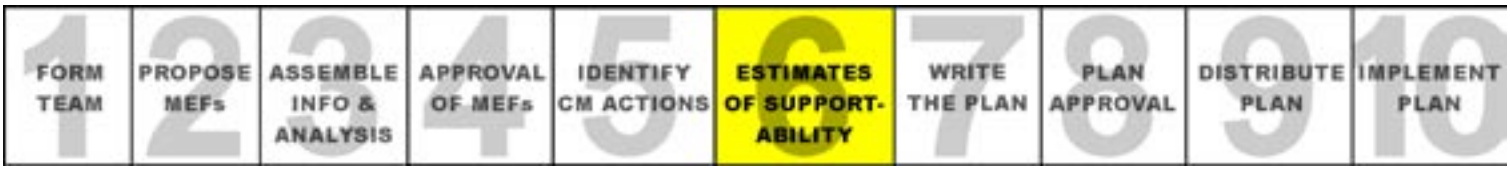
This coordination of changes uses information from the various analysis conducted earlier and categorizes the full impact of change across the organizational enterprise. The five areas matrixed to identify where change will impact the operation include:

- Policy,
- Operational Processes and Organization,
- Training and Education,
- Procurements and Investments, and
- Support Services.

When developing the draft CM Plan, planners also create courses of action (COA) to support the plan. Each COA will present an integrated approach addressing all pertinent categories of the issue. This analysis matrix provides the decision maker with a disciplined methodology to understand the full implications of the COA before deciding which best supports the intent of the plan. In addition, the analysis forms the basis of the implementation actions to be carried out once the plan is approved. Part IV of this Planning Guide discusses CM Plan Implementation in more detail.

For example, a base or station may decide to install back-up data systems for critical information as a remediation step during CM Plan development. Planners will consider and take action regarding the impact on:

- Policy: Implementation will require all users to maintain critical data on a shared drive.
- Operational Processes and Organization: Organization will assign one person to manage the data management system, and based on operational requirements, will back up the data three times per week
- Training and Education: Organization must select and train one person to serve as the alternate data management system (DMS) operator; all users of the critical data require 8 hours of class/practical instruction on how to operate the system.
- Procurements and Investments: In addition to the software, DMS requires the procurement of one server, two backup tape drives, and an additional mount to install the system.
- Support Services: DMS requires an annual software license fee.

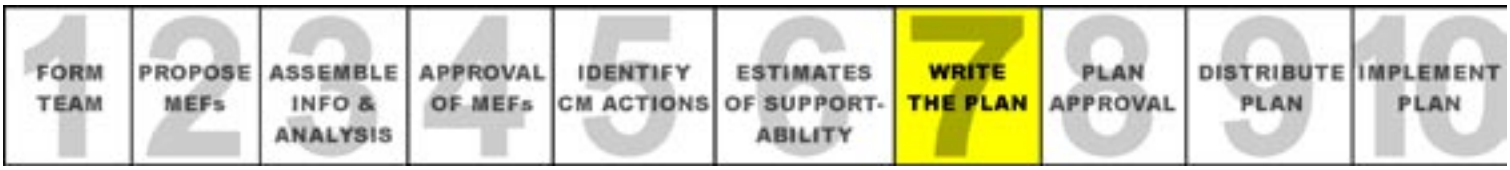


STEP 6. ESTIMATES OF SUPPORTABILITY

This Step seeks concurrence from the staff for the proposed CM concept of operations and all CM requirements actions. The staff estimates of supportability provide a logical and orderly examination of all factors affecting, and affected by, the CM concept. Regardless of the level of informal staff review that occurs, the completed list of CM requirements is staffed in a more formal manner to ensure the actions:

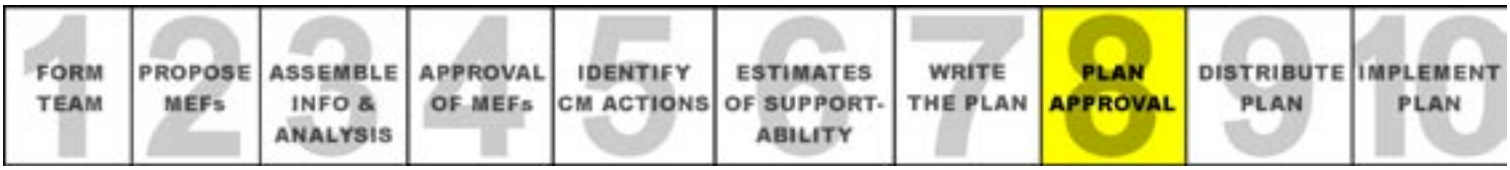
- Are Achievable
- Are Affordable, and that there are no
- Unintended Consequences

The staff reviews the proposed actions and determines if they are supportable. If not supportable the staff indicates alternatives to the team recommendations. Un-supportable actions and recommended alternatives will be subject to the same coordinated review that took place in Step 5, and submitted for staff review until an achievable concept of operations is reached.



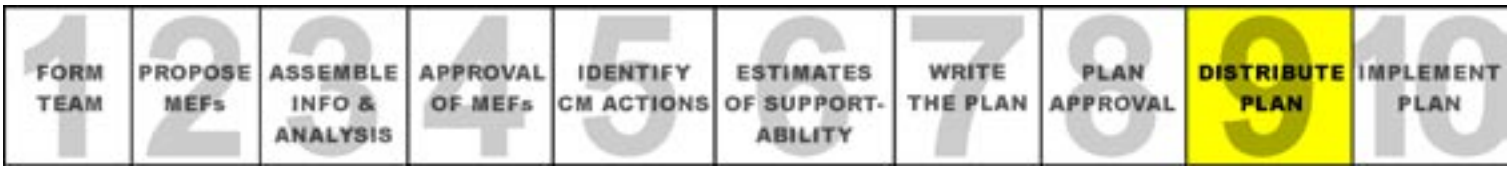
STEP 7. WRITE THE PLAN

This Step brings all of the actions identified in Step 5, and reviewed in Step 6, together in a written Plan. Appendix C contains a list of characteristics of a well-written CM plan, and serves as a checklist to guide planners in developing their plan. Appendix D provides planning considerations within all 15 functional areas across the four phases of an event. Appendix E is a notional CM plan format; however the best format is the one that meets the requirements of your organizational structure. Regardless of format, it is important that the Plan addresses each Phase and identifies responsibilities for each action.



STEP 8. PLAN APPROVAL

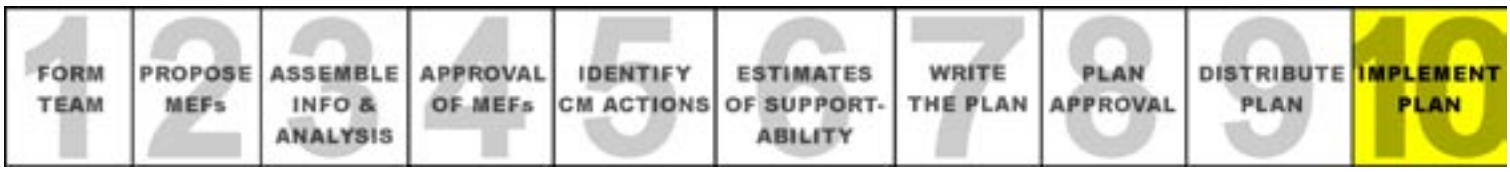
This Step involves presentation of the Plan to senior leadership for review and approval. The CM team leader should emphasize the importance of leadership familiarity with all provisions of the CM Plan, and in particular those actions in which leadership has an active role.



STEP 9. DISTRIBUTE THE PLAN

This Step involves publication and distribution of the Plan, and ensuring everyone in the organization is aware of its provisions and how to obtain access to it. Physical distribution plans, in paper, CD ROM, or intranet formats, should also consider providing a means to access the Plan after working hours, and assume that electronic access may be lost as a consequence of an event. Personnel with key roles set forth in the plan might consider maintaining copies outside the

workplace (residence, personal vehicle, etc). The distribution plan should also consider who outside the organization may require a copy, and how to safeguard any classified information the plan may contain or refer to.



STEP 10. IMPLEMENT THE PLAN

Implementation begins with the approval, publication and distribution of the plan and continues until an event occurs. Implementation includes:

1. Acting on recommendations made during the vulnerability assessments and other analysis,

2. Incorporating the plan throughout operations and culture,

3. Conducting familiarization and proficiency training,

4. Procuring, distributing and maintaining equipment and systems contained in the plan, and

5. Exercising, evaluating and updating the plan. Part III discusses implementation in more detail.

PART III:
IMPLEMENTATION

Part III: Implementation

Publishing a CM Plan is a significant milestone in the CM process, but much work remains for the planner. Using the same format as the Part II (Planning) discussion of the five areas where change impacts the organization, this section discusses how CM Plan implementation affects an organization:

- Policy,
- Processes and Organization,
- Training and Education,
- Procurement and Investments, and
- Support Services.

THE CONSEQUENCE MANAGEMENT IMPLEMENTATION PLAN

The purpose of an Implementation Plan is to provide the organization with the means to maintain the plan's validity and currency, while remaining ready to execute the plan should an event take place. Additionally, an implementation plan can facilitate a smooth transition back to the Pre-event phase at the conclusion of an event. There is no particular format to document the requirements comprising CM Plan implementation. Checklists, execution matrices, as well as more formal implementation directives are all methods of identifying the who, what, why and when aspects of implementing the plan, and providing commanders with a means of tracking progress.

Concurrent with writing the CM Plan, the staff develops implementation planning steps (see Part II). These documents usually include a Plan of Action and Milestones for fielding new equipment, publishing new policies, or changing processes necessary to incorporate the CM plan into the organization's other processes. The implementation plan is the commander's and planner's tool for ensuring all elements and requirements of the CM Plan are actually satisfied.

POLICY: Adapting a CM Plan may impact the high-level plans, strategic goals, and operating procedures of the organization. Based on the plans content, the organization should review specific and/or general policies in order to develop the best course of action and methods to integrate CM into the organization as a way of doing business rather than an additional cost of doing business. Examples of how CM impacts policy include:

- Recall and accountability criteria
- Use of alternate sites
- Limitations on procurements
- Requirements for 24x7 availability of key personnel
- Process for managing disruptive events

PROCESSES AND ORGANIZATION: Given the nature of military operations, the most visible impact of implementing a CM Plan occurs within processes and organizations.

Drawing from issues within the CM Plan, organizations modify or "re-engineer" their processes to strengthen them against disruption, build in redundancy, and achieve a better posture to execute the plan, while increasing their efficiency to transition back to normalcy after an event.

The organization also provides a line of defense against disruption. Changes here may reflect assignment of full time personnel to CM duties, designating and training members of the staff as various CM teams, or increasing the use of dispersion and other tactics to reduce the exposure to an event.

Understanding and adapting to processes in the external environment strengthen the organization's resiliency and posture for surviving disruptive or catastrophic events. Where possible, partnering with other public and private agencies for CM Plan implementation leverages best practice benefits against cost concerns across the enterprise.

TRAINING AND EDUCATION: While processes and organizations are the most visible embodiments of incorporating CM into the organizational culture, training and education are clearly the most important. Educating members of the organization ensures a uniform understanding of concepts, procedures, and policies contained in the CM Plan, while training increases both mental and physical proficiency in executing the CM plan while developing an appreciation for the friction and uncertainty one will encounter during an actual event. To this end, training exercises - with their associated lessons learned - are crucial to fully implement the plan.

Tables III-1 through III-3 provide training and exercise recommendations.

Procurement and Investments: Implementing a CM Plan will to some extent require expenditures necessary to outfit the organization and the people with the equipment, systems, and capabilities necessary to execute the plan. In addition to standard investment costs, planners should also be aware of life-cycle costs, retirement costs, and associated training and maintenance costs, as well as the requirement for interoperability with external supporters and systems.

Support Services: These services include not only the professional, maintenance, administrative, etc, services necessary to keep the organization in operation, but also those services specific to CM, such as data backup, alternate sites, security, etc.

CONSEQUENCE MANAGEMENT EXERCISES

Exercising the plan serves many purposes. It creates familiarity with the actions listed in the plan, identifies any gaps or disconnects in the plan, and helps reinforce CM as integral to the organization's way of conducting day to day operations. Appendix F contains sample exercise scenario formats.

Exercises should progressively test participant ability to implement the actions contained in the plan, as well as inject increasingly complex scenarios into the exercise play. The following tables list, in skill progression order, recommended exercise topics within each of the three component sections of a CM program.

COMPONENT FOCUS AREA: PEOPLE

EXERCISE EVENT	PURPOSE
Personnel Accountability	*Ensure personnel within the organization understand personnel accountability processes and their responsibilities to maintain and report accountability*
Personnel Recall Rosters	*Ensure recall rosters accurately reflect personnel within the organization*
Phone Recall	*Validate the accuracy of the published recall numbers by calling personnel within the organization*
Tabletop Recall Discussion (Chalk Talk)	*Ensure personnel know the procedures and responsibilities prior to conducting an actual recall*
Partial Recall	*Test the recall procedures using a selected sample of the organization*
Total Recall (Work Place)	*Fully test the procedures necessary to recall personnel to the business workspaces*
Recall (Alternate Location)	*Fully test the procedures necessary to recall personnel to the businesses' alternate workspaces*
Periodic Evacuation of Building (Fire Drill)	*Maintain the personnel accountability skills associated with evacuation*
Shelter-in-Place	*Demonstrate actions necessary to shelter the workforce in place*

TABLE III-1

Component Focus Area: Connectivity

Exercise Event	Purpose
During Hours System Access	*Ensure full access to data backup systems during working hours*
After Hours System Access	*Ensure full access to data backup systems after working hours*
Automated Backup System Check	*Ensure backup systems are operating*
Use of Backup Server during Normal Working Hours	*Validate the quality of backed up data by using this data during normal working hours*
Backup Server Power Support	*Ensure backup systems have adequate power supply*
Validate Assignment of Laptops, Blackberries, etc.	*Ensure proper assignment of portable data systems*
Remote System Access Checks for Designated Personnel	*Ensure designated personnel are able to access their work from an alternate location*
Full Spectrum Data Accessibility via Dial-In	*Ensure personnel can remotely access the full spectrum of data normally accessible at their office workstation*
Multi-day Use of Dispersal Techniques (Telecommute)	*Ensure sustained connectivity from multiple locations, while developing the procedures and techniques to manage a dispersed workforce*

TABLE III-2

Component Focus Area: Execution

Exercise Event	Purpose
Partial Home Base Execution (Select Individuals)	*Exercise the full spectrum of CM activities (evacuation, personnel accountability, remote access to backup data by selected members of the organization dispersed to their residences)*
Partial Alternate Site Execution (Select Individuals)	*Exercise the full spectrum of CM activities (evacuation, personnel accountability, remote access to backup data by selected members of the organization dispersed to their alternate sites)*
Total Home Base Execution (One-Day Event)	*Exercise the full spectrum of CM activities (evacuation, personnel accountability, and sustained remote access to backup data by the entire organization after dispersing to their residences)*
Home and Alternate Site Execution (One-Day Event)	*Exercise the full spectrum of CM activities (evacuation, personnel accountability, and sustained remote access to backup data by the entire organization after dispersing to their residences and alternate sites)*
Home and Alternate Site Execution (Multi-Day Event)	*Exercise the full spectrum of CM activities (evacuation, personnel accountability, and sustained remote access to backup data by the entire organization after dispersing to their residences and alternate sites)*

TABLE III-3

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)

NIMS is a national-level management tool that provides a consistent approach for Federal, State and local governments to work effectively together to prepare for, respond to, and recover from domestic incidents. NIMS incorporates best practices currently in use by incident managers, and will continue to evolve to incorporate new concepts, processes and protocols over time.

An essential element of NIMS is the Incident Command System (ICS). ICS is a management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel procedures, and communications operating within a common organizational structure. Understanding ICS and how it will influence an external response to events affecting DON property, people, and facilities will benefit DON CM managers.

Commanders should consider use of the ICS methodology in developing internal event management processes. ICS works because it is based upon basic management skills that managers already know and use.

More on NIMS can be found at the Department of Homeland Security website:

http://www.dhs.gov, and the FEMA web-site: http://www.fema.gov.

APPENDIX A: COMMANDER'S CIP PLANNING WORKSHEET

Appendix A: Commander's CIP Planning Worksheet

This worksheet assists planners in validating their CM requirements by developing and ranking each Mission Essential Function (MEF) of the installation, identifying the relative contribution each Functional Area (FA) makes to the MEF, and identifying the Critical Assets necessary to produce or support the MEF. Additionally, this worksheet assists the Naval Integrated Vulnerability Assessment team in focusing their preparations on MEFs, Critical Assets, and dependencies that are important to the commander.

MISSION

The installation Mission Statement is a logical point of departure for completing the worksheet. However, many Mission Statements are out of date and no longer reflect the actual missions as they exist today. Additionally, this worksheet focuses only on those missions that apply to the strategic, operational, and tactical requirements of the installation "customers."

MISSION ESSENTIAL FUNCTIONS (MEFS)

Identifying MEFs is where practical Critical Infrastructure Protection really begins. The true value of infrastructure stems from its use, rather than its existence. Protecting critical infrastructure's availability for use, and its ability to function as intended, contributes to Continuity of Operations and supports Mission Assurance. MEFs are those processes that generate the strategic value of an organization; MEFs achieve the mission of the installation. A single mission may have multiple MEFs. The loss or disruption of these MEFs results in immediate degradation to the output of the organization, and causes immediate negative impact to the organization's customers.
All MEFs have certain characteristics.

- They are **"strategic" in nature** – they promote the mission of the organization.
- They **generate significant value** to your customers.
- Their interruption or **loss has an immediate impact** on your customer's ability to perform their tasks.

As an informal approach to developing an understanding of MEFs, ask yourself, "What is the purpose of our organization?" "If our organization could do but one thing, what would it be?" "What gives the most value to our customers?" and, "If we ceased operations, what loss of support would hurt our customers first, and the most?"

The answers to these questions form the outline of your MEFs.

MEFs may contain one or more Functional Area components (see FA discussion below), and may involve one or more organizational elements of the installation. Last, MEFs must be sufficiently detailed for planners to grasp the root activities that make up the function. MEFs answer the "who, what, when, and where" questions; the Consequence Management Plan addresses the "how." Given the installation mission of "Provide Fleet Support," examples of MEFs might include the following:

Poor example of a MEF: "To provide Fleet support."

Better example of MEFs:

MEF 1: "To provide pier-side support to home ported and visiting US Navy vessels."

MEF 2: "To provide harbor control operations."

Best example of MEFs:

MEF 1: "To provide pier-side support to home ported and visiting US Naval vessels, including fuel, utilities, water front security, and cargo handling."

MEF 2: "To provide limited intermediate ship repair to home ported and visiting US Naval vessels."

MEF 3: "To provide harbor control and operations to support the fleet's ability to sortie within two days in support of Combatant Commander initiatives."

CATEGORIZATION OF FUNCTIONAL AREA (FA) IMPORTANCE TO MEFS

The categorization of FAs is characterized by few absolutes, and a strong working knowledge of the organization's MEFs and internal processes within the 15 FAs is required. When categorizing FAs, consider the FA's contribution to the MEF in the "normal" Pre-Event Phase -- before a disruptive event occurs. While the importance of various FAs may vary during and after a disruptive event, identifying the importance of an FA in the Pre-Event Phase provides a baseline from which to conduct Disaster Preparedness planning and exercises, enter into support agreements, etc. Considering single points of failure or possible alternative means of providing support within an FA serves to divert focus from establishing the baseline Pre-Event conditions and is not part of this worksheet.

THE 15 FUNCTIONAL AREAS:

1. **COMMAND AND CONTROL** includes the people and procedures necessary to sustain leadership's ability to maintain situational awareness of on-going events while exercising leadership decision making processes, etc.

2. **OPERATIONS** include production, planning, R&D, sales, marketing, partnerships, outreach, commitments listed in Memorandums of Understanding or Agreements, and other inter- or intra-relationships, etc.

3. **HUMAN RESOURCES AND PUBLIC RELATIONS** include recall, points of contact, alternate Human Resources sourcing, training, Freedom of Information Act (FOIA) issues, recruiting, identification, skill sets, and Media Relations, etc.

4. **SECURITY** includes physical and cyber security, security clearances, safeguarding classified or proprietary documents and equipment, surveillance and intrusion detection equipment, escorts, traffic control and routing, Chemical Biological Nuclear Radiological and Explosive (CBNRE) detection equipment, and coordination with local, State, or Federal security and law enforcement officials, etc.

5. **COMMUNICATIONS** include mass notification systems, all telecommunications (landline and portable), mobile radio, and facsimile transmissions, etc.

6. **FACILITIES** include physical structures, identification of alternate facilities, parking, health and comfort requirements, office furniture, etc.

7. **UTILITIES** include electrical power, water, Heating Ventilation and Air Conditioning (HVAC), fuel, utility sourcing, alternate providers, etc.

8. **OPERATIONAL EQUIPMENT** includes business-generation equipment (e.g.: production line), transportation, and detection equipment for Hazardous Material (HazMat), etc.

9. **TRANSPORTATION** includes passenger, cargo, heavy equipment transporters, traffic flow, and interaction with local, state, or Federal movement control agencies, etc.

10. **SUPPORT SERVICES** include contracted services, service provider organizations, and alternate sources of services, and possible outsourcing for lost or diminished capabilities, etc.

11. **INFORMATION TECHNOLOGY/INFORMATION SYSTEMS (IT/IS)** includes all aspects of IT/IS support and processing capabilities to include communication, networking, data management, analysis, operating systems, applications, peripherals, system certification, hardware, software, IT maintenance and services, etc.

12. **FISCAL, CONTRACTING, AND PURCHASING** includes funding estimates for incident response and recovery preparation that impacts the MEF, to include the processes to request, authorize and expend funds in support of the MEF.

13. ENVIRONMENTAL, HEALTH AND SAFETY includes all medical services, Occupational Safety and Health Administration (OSHA) compliance requirements, infrastructure, Human Resources and capabilities supporting the MEF.

14. FIRST RESPONDERS includes local fire and rescue, hazardous material response, law enforcement, and mechanisms and procedures to tap into State and Federal responders.

15. LEGAL includes insurance, liability, governance, labor relations, contract issues, regulatory compliance, etc.

Importance: The importance of a FA is determined by its contribution to enabling and sustaining the organization's MEFs. The worth, contribution, or criticality of a particular FA is determined by that organization using the following five criteria.

Critical: MEF ceases upon loss of FA

High: Significant FA contribution to MEF performance

Medium: Moderate FA contribution to MEF performance

Low: Minimal FA contribution to MEF performance

None: The FA has does not contribute to MEF performance

Critical: The MEF relies on the FA to the extent it can not be carried out if the capabilities or processes within the FA are lost or degraded.

Example: An organization's MEF of loading ammunition aboard pier-side shipping is totally reliant on electricity to operate MHE. No other possible means exist to perform the function. The UTILITIES FA would therefore likely be assessed as CRITICAL.

High: The functional area provides significant contributions to the MEF such that functional area loss or degradation will result in a proportionate degradation to the MEF.

Example: Using the scenario in Example #1, the ammunition loading function can be carried out without electricity but at a rate 40% slower than when electricity is available. This potential degradation in MEF performance would likely result in an assessment of HIGH within the UTILITIES FA.

Medium: The functional area supports the MEF yet its contribution to MEF processes do not result in total MEF failure upon their loss.

Example: The HUMAN RESOURCES/PUBLIC RELATIONS (HR/PR) FA supports the MEF described in Example #1 by providing trained personnel of various occupational skills. Some skill sets require critical/low density personnel, or require special training, but may be resourced within organic capabilities with moderate disruption to the MEF. HR/PR would therefore likely be assessed as MEDIUM importance.

Low: The functional area provides minimal contribution to MEF performance and its loss would have an equally minimal impact on the MEF.

Example: Pier-side ammunition loading is supported by an automated process that forecasts load times, personnel requirements, and movement routes. Loss of the automated tool would have little impact on the organization's ability to actually load ammunition aboard pier-side shipping, therefore the FA of INFORMATION TECHNOLOGY / INFORMATION SYSTEMS (IT/IS) would be evaluated as LOW in importance.

None: The functional area does not support the MEF and its loss will have no impact on MEF performance.
Example: Loss of LEGAL services has no impact on the organization's ability to perform pier-side ammunition loading operations.

CRITICAL ASSETS

There are assets that are critical to generating or sustaining each MEF. For the purposes of this worksheet, these are the Critical Assets without which the MEF suffers unacceptable degradation or disruption. The importance of an asset at the DON, DOD, or National level does not impact its listing on this worksheet; again, focus on those assets necessary to generate or sustain each MEF.

The 15 Functional Areas found in the worksheet provide a useful framework within which we consider Critical Assets. A single infrastructure asset may support multiple functions that may or may not be critical. The support of multiple functions by a single infrastructure asset does not in itself generate critical asset status. This worksheet is concerned only with those assets supporting those functions that are critical to the mission of the installation. Understand that not every FA will generate a Critical Asset, and some Critical Assets may support more than one MEF.

Example: Given the following MEF, "Receive, store, and issue ammunition," critical assets may include MHE, bunkers, utilities, inventory tracking systems, ammunition handlers, etc., while assets such as billeting and MWR facilities have no role in this particular MEF.

DEPENDENCIES

Internal or external ownership, often dictates the nature of how a capability integrates into the MEF. Internal capabilities are those that the MEF owner owns and may employ without prior coordination. An example of this would be the Installation Security Force, or the Headquarters Command and Control capabilities. External capabilities are those that do not directly belong to the commander, and whose employment requires prior coordination and authorization beyond that of the MEF's owner. Examples may include tenant command services (Federal Fire Department), private sector commodities such as utilities, services such as equipment repair, or service providers such as NMCI.Instructions:

NOTE: Steps 1, 2, and 3 are completed in sequence (complete all steps 1, then all steps 2, and finally, all steps 3).

Step 1. Consider the most important missions of the installation (the reasons why your installation exists). Consider the contribution your organization makes to the strategic, operational, and tactical requirements of your customers (those

who rely on your value), what inputs you need to perform your functions, and what 30-day impact the disruption of your installation would have on your customers. There are typically three to five missions/reasons why an installation exists. Using a separate worksheet for each, list the Mission/Reason for Existence in Block 1.

Step 2. In Block 2, list in detail the specific functions essential to either generate or support each mission/reason for existence listed in Block 1. If a mission has multiple discrete MEFs, use a separate worksheet to list each MEF (being sure to include the mission/reason for existence in Block 1).

Step 3. Considering all the MEFs, In Block 3 rank each MEF by its importance, 1 through "X."

Example: Your installation has three Missions. Mission 1 has two MEFs; Mission 2 has four MEFs; Mission 3 has one MEF. You will have seven total worksheets (one per MEF), with worksheets one and two containing the two MEFs for Mission 1, worksheets three through six containing the four MEFs for Mission 2, etc.

NOTE: Complete steps 4, 5, and 6 for each worksheet before moving to the next (complete step 4, 5, and 6 on one page, then move to the next page).

Step 4. In Block 4, circle the criteria listed under each Functional Area (FA) that best describes the FA's contribution to enabling and/or sustaining the MEF in question. The importance of a FA may vary from worksheet to worksheet depending on its contribution to a particular MEF. If the FA has no contribution, circle "none."

Step 5. Considering each FA, list in Block 5 any and all Critical Assets associated with the MEF. There need not be a Critical Asset associated with every FA.

Step 6. For each Critical Asset listed in step 5, list in Block 6 the internal or external dependencies of each Critical Asset, noting whether the dependency is internal (I), or external (E).

Step 7. Have the Commander initial and date each page.

Step 8. Insert appropriate Classification Marking – Unclassified, Confidential, Secret, Top Secret – and safeguard as required.

(_____

INSERT CLASSIF

COMMANDER'S CRITICAL INFRASTRUCTU

1. MISSION/REASON FOR EXISTENCE	2. MISSION ESSENTIAL FUNCTION	4. FUNCTIONAL AREA CRIT (Circle One)
		Command and Control: Critical High Medium L
		Operations: Critical High Medium L
		HR/Public Affairs: Critical High Medium L
		Security: Critical High Medium L
		Communications: Critical High Medium L
		Facilities: Critical High Medium L
		Utilities: Critical High Medium L
		Equipment: Critical High Medium L
		Transportation: Critical High Medium L
		Services: Critical High Medium L
		IT/IS: Critical High Medium L
		Finance, Contracts, Purchas Critical High Medium L
		Environmental, Health and Sa Critical High Medium L
		First Responders: Critical High Medium L
	3. RANK	Legal: Critical High Medium L

NOTE: USE A SEPARATE FORM FOR EACH MISSION/REASON FOR EXISTENCE

(_____

INSERT CLASSIF

_____)

ICATION MARKING

URE PROTECTION PLANNING WORKSHEET

TICALITY	5. ASSOCIATED CRITICAL ASSETS	6. INTERNAL/EXTERNAL DEPENDENCIES
ow None		
ow None		
ow None		
Low None		
ow None		
Low None		
ow None		
ow None		
ow None		
ow None		
ow None		
ing: ow None		
afety: ow None		
ow None		
ow None		

7. COMMANDER'S INITIALS: _____ DATE: _____

_____)

ICATION MARKING

APPENDIX B: RISK ASSESSMENT & ANALYSIS TOOLS

Appendix B: Risk Assessment & Analysis Tools

Risk assessment identifies and analyzes threats to and vulnerabilities of MEFs and the potential impact of the loss or degradation of MEFs. Threats are those things which may actually cause the disruption, whether intentionally or accidentally, through acts of nature or man-made. Threat assessments evaluate the likelihood and degree to which an event may occur within a specified timeframe. Vulnerability assessments identify internal and interdependency weaknesses that can be exploited to adversely affect the continuity of operations with the MEFs. Business Impact Analysis (BIA) provides a means of measuring the effects of a disruptive event in terms of loss and/or downtime of selected MEFs. Decision Analysis, like a Business Impact Analysis, provides an analytical tool to measure trade-offs in establishing recovery point options and plans.

Risk is often expressed in terms of Annualized Loss Exposure, or ALE, which is a quantitative means of assessing a MEF's relative importance or ranking in those cases where MEF outcomes are highly objective in nature. ALE can be determined using loss controls already in-place, and can also be forecast by assuming additional mitigation or remediation is conducted. Qualitative, subjective factors almost always enter into risk analysis to measure intangibles inherent in MEFs, and these tools provide but one means to assist planners in weighting MEF values.

Vulnerability Assessments, Business Impact Analysis, and Decision Analysis are introduced below.

CONDUCTING A VULNERABILITY SELF-ASSESSMENT

It is critical in the CM planning process that a vulnerability assessment be conducted and remediation be carried out. Unfortunately, not all vulnerabilities can be specifically and directly remediated. For example, resource constraints may lead decision makers to accept some level of risk rather than improving each asset to achieve complete invulnerability. Therefore mitigating actions must be identified and integrated into the CM Plan. A sample chart to use in analyzing vulnerabilities is provided as Table A-1.

TYPE OF EMERGENCY	Probability	Human Impact	Property Impact	Operational Impact	Internal Resources	External Resources	TOTAL
Score	HIGH 5			LOW 1	WEAK 5	STRONG 1	

THE LOWER THE SCORE THE BETTER

TABLE A-1. VULNERABILITY ANALYSIS CHART

LIST POTENTIAL EMERGENCIES

In the first column of the chart, list emergencies that could affect your organization, including those identified by your local emergency management office. Consider both:

- Emergencies that could occur within your organization
- Emergencies that could occur in your community

Following are some other factors to consider:

(a) Historical — What types of emergencies have occurred at this organization, at other facilities in the area, and in the community?

- Fires
- Severe weather
- Hazardous material spills
- Transportation accidents
- Earthquakes
- Hurricanes
- Tornadoes
- Terrorism
- Utility outages

(b) Geographic — What can happen as a result of the organization's location? Keep in mind:

- Proximity to flood plains, seismic faults and dams
- Proximity to companies that produce, store, use, or transport hazardous materials
- Proximity to major transportation routes and airports
- Proximity to nuclear power facilities

(c) Technological — What could result from a process or system failure? Possibilities include:

- Fire, explosion, hazardous materials incident
- Safety system failure
- Telecommunications failure
- Computer system failure
- Power failure
- Heating/cooling system failure
- Emergency notification system failure

(d) Human Error — What emergencies can be caused by employee error? Are personnel trained to work safely? Do they know what to do in an emergency? Human error is the single largest cause of workplace emergencies and can result from:

- Poor training
- Poor maintenance
- Carelessness
- Misconduct
- Substance abuse
- Fatigue

(e) Physical — What types of emergencies could result from the design or construction of the facility?

Does the physical facility enhance safety? Consider:

- The physical construction of the facility
- Hazardous processes or byproducts
- Facilities for storing combustibles
- Layout of equipment
- Lighting
- Evacuation routes and exits
- Proximity of shelter areas

(f) Regulatory — What emergencies or hazards are you regulated to deal with? Analyze each potential emergency from beginning to end. Consider what could happen as a result of:

- Prohibited access to the facility
- Loss of electric power
- Communication lines down
- Ruptured gas mains
- Water damage
- Smoke damage
- Structural damage
- Air or water contamination
- Explosion
- Building collapse
- Trapped persons
- Chemical release

ESTIMATE PROBABILITY

In the Probability column, rate the likelihood of each emergency's occurrence. This is a subjective consideration, but useful none the less. Use a simple scale of 1 to 5 with 1 as the lowest probability and 5 as the highest.

ASSESS THE POTENTIAL HUMAN IMPACT

Analyze the potential human impact of each emergency — the possibility of death or injury. Assign a rating in the Human Impact column of the Vulnerability Analysis Chart. Use a 1 to 5 scale with 1 as the lowest impact and 5 as the highest.

ASSESS THE POTENTIAL PROPERTY IMPACT

Consider the potential property for losses and damages. Again, assign a rating in the Property Impact column, 1 being the lowest impact and 5 being the highest. Consider:

- Cost to replace
- Cost to set up temporary replacement
- Cost to repair

ASSESS THE OPERATIONAL IMPACT

Consider the potential impact on your ability to sustain your MEFs. Assign a rating in the Operational Impact column.

Again, 1 is the lowest impact and 5 is the highest. Assess the impact of:

- Interruption of the operational process.
- Personnel unable to report to work
- Customers unable to reach facility
- Interruption of critical supplies
- Interruption of product distribution

ASSESS INTERNAL AND EXTERNAL RESOURCES

Next assess your resources and ability to respond. Assign a score (from 1 to 5) to your Internal Resources and External Resources. The lower the score the better. To help you do this, consider each potential emergency from beginning to end and each resource that would be needed to respond. For each emergency ask these questions:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to us for this emergency as quickly as we may need them, or will they have other priority areas to serve? Consider the require ment for external resources to also support such large-scale events producing mass casualties or wide spread destruction of infrastructure.

If the answers are less than a 5, identify what can be done to correct the problem. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish mutual aid agreements
- Establish agreements with specialized contractors

ADD THE COLUMNS

Total the scores for each emergency. The lower the score the better. While this is a subjective rating, the comparisons will help determine planning and resource priorities.

BUSINESS IMPACT ANALYSIS

A BIA can assist planners in determining how to plan for recovering MEFs in terms of time and cost, and avoid excessive expenditures of resources in recovering capabilities before or beyond the extent they are actually needed. Many of the objectives of a BIA are incorporated in the planning methodology defined in this Planning Guide (e.g. MEF identification), however the BIA includes analytical tools to measure actual effects of a disruption and the ensuing recovery actions. BIA objectives are to:

- Identify MEFs and their interdependencies
- Determine the priority for recovery for MEFs
- Determine recovery time objectives and recovery point objectives
- Determine the actual impact to MEFs, either financial or by other metrics

The steps necessary to identify and prioritize MEFs have been discussed earlier in the Guide. Forms A-1 and A-2 at the end of this Appendix provide a means of documenting MEF information. The detailed analysis now looks at how long each MEF could be unavailable to the organization, and the point in time to which it must be restored.

RECOVERY TIME AND RECOVERY POINTS

Recovery Time is the restoration goal to be met from loss of the MEF until its recovery, sometimes called the Recovery Time Objective (RTO). The recovery point, or Recovery Point Objective (RPO), usually refers to data recovery in terms of the point in time to which data must be recovered. It may also refer to non-data specific processes which, if not maintained continuously, could result in recovery costs disproportionate to the cause. An example may be loss of aircraft maintenance systems due to caustic chemicals pooling in the equipment after a simple power failure. In general, the longer a RTO for any MEF the less it will cost to *recover*, however, the corresponding losses associated with MEF unavailability will cause losses to increase exponentially. Figure A-1 represents the cost of recovery, while Figure A-2 reflects losses due to the time a MEF is unavailable.

Overlaying the curves in Figures A-1 and A-2 indicates the point where loss equals cost of recovery and represents the initial restoration point for the MEF (Figure A-3). By determining the cost-benefit curve for each MEF restoration, the planner can apply subjective analysis in determining additional vulnerability mitigation factors to include based on MEF prioritization. The costs of additional mitigation factors compared to overall losses due to disruption of MEFs provides initial, subjective, recovery goals. The CM planner should consider residual risks and cost/loss impact when assessing MEFs and individual functional areas, and consider aggregate loss exposures when developing courses of action for vulnerability mitigation and recovery strategies.

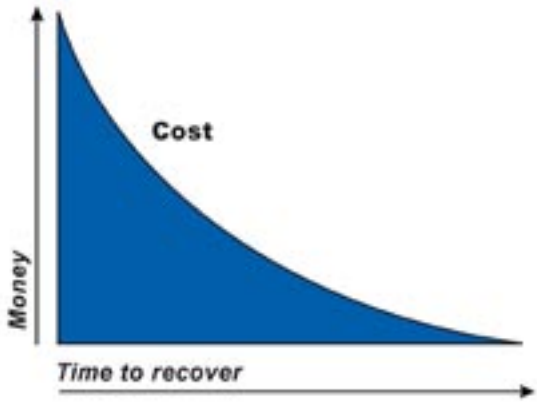


FIGURE A-1

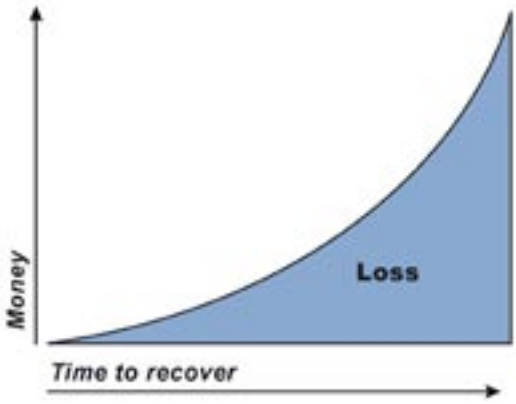


FIGURE A-2

Forms A-1 and A-2 are sample tools to assist in prioritization of MEFs based upon relative value and allowable disruption times.

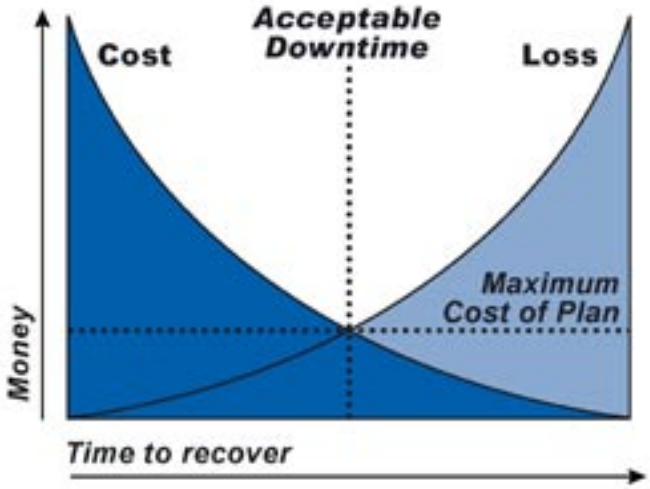


FIGURE A-3

DECISION ANALYSIS

Risk Assessment is a systematic process of documenting and weighing alternative scenarios in terms of their respective probabilities of success or failure, costs, and benefits. It enables a decision making team such as the CM Planning Team to examine decisions in a structured and efficient manner.

Using a Decision Analysis Table, such as the Notional Decision Analysis Table depicted in Table A-2, a decision-making team can systematically map out available options and their potential outcomes (e.g. the scenario or decision analysis table). Once completed, the team can then estimate the absolute or relative probabilities and benefits of each scenario.

This systematic, visible approach helps to focus the decision-making team. It makes visible the information needs and clearly documents the elements that have been considered along each scenario. In many cases, completion of this process on a subjective level will clearly identify the appropriate decision path. In other cases, quantitative assessment is required to identify the best path from a mathematical perspective.

Decision analysis requires quality input information. Qualified people with experience in the area in which the decision is being made should be consulted for input and data.

The notional Decision Analysis Table (Table A-2) uses three scales to establish the inter-connections between the MEF, the impact of the event on the MEF, and the possible responses to the impact. In this example, the notional MEF "Communications" is inoperable due to a disaster event.

Table A-2 Notional Decision Analysis Table

Response, Recovery or Reconstitution Phase (as appropriate)						
MEF Functional Title # (e.g.) Communications						
Time required to complete proposed actions:						
Proposed Actions:	< 1 hr	> 1 hr < 4 hr	> 4 hr < 8 hr	> 8 hr < 24 hr	> 24 hr < 28 hr	< 48 hr > 96 hr
1. Restore Partial Capability	B	C	C	D	D	D
2. Restore Full Capability	A	C	C	C	D	D
3. Activate Backup Unit	A	A	A	A	D	D
4. Shift Responsibility to Backup Unit	A	A	A	A	D	D

First, the horizontal scale may contain any appropriate measure (time, personnel, cost, etc.) as determined by the command. In this example, the scale reflects time periods from 1-96 hours.

Second, the vertical scale on the left reflects the proposed actions (numbered 1 through 4 in this example) in response to the event and its impact on the critical asset and its MEFs.

Third, an impact assessment scale (Table A-3) is used to complete the table in order to express the overall impact that the event has on the MEF.

Table A-3 Impact Assessment Scale

A	No Impact
B	Minimum (Minimum interruption of function or capability)
C	Significant (Moderate degradation of function or capability)
D	Critical (Loss of function or capability)
E	Catastrophic (Cessation of Business Operations)
F	Unacceptable (Strategic loss or failure)

Each individual asset owner should determine the unique content and weight of their scale to express the particular nature of the critical asset's specific MEFs.

Business Impact Analysis

Form 1: Identify All Mission Essential Functions

Functional Area: _____

Mission Essential Function	MEFS # **	MEFS Owner	Other Stakeholders	Weight*

Form A-1

Mission Essential Function Identification

Weight: relative subjective value from 1 (critical) to 5 (not critical)

***** Assign each MEF a number corresponding to Functional Area, e.g. MEF # 2F is the second numbered MEF within the Fiscal Functional area***

Business Impact Analysis

Form 2: Weighted MEF Assessment

Functional Area: _____

MEFs # *	Dependent on MEF#s	Critical Assets Supporting MEFs	Maximum Allowable Disruption Time*

Form A-2

Weighted MEF Assessment

**** Enter MEFs in prioritized order based on Form #1 weighting and subject analysis of MEF importance to the enterprize***

***** Estimate maximum time MEF can be in a disrupted state without exceeding acceptable loss thresholds***

APPENDIX C:
CM PLAN CHARACTERISTICS

Appendix C: CM Plan Characteristics

The following is a checklist of common elements comprising CM programs and plans. The checklist is useful in developing and evaluating CM plans and programs and conducting CM program self-assessments.

SECTION A: CM PROGRAM

1. Has the command established a formal CM Program?
2. Does the program focus on preserving MEFs?
3. Does the program identify MEFs?
4. Does the program prioritize MEFs?
5. Does the CM Program designate a CM officer?
6. Does the CM Officer have the following pre-event responsibilities: CM program management; Planning; Implementation; Tests, Training, and Exercises?
7. Does the CM Officer have programmatic responsibilities during plan execution?
8. Does the organization have an established CM governing body?
9. Does the organization's governing body have a charter?
10. Does the organization's governing body consist of cross-department membership?
11. Does the organization's governing body conduct periodic scheduled meetings?
12. Does the organization's governing body have decision making authority?
13. Does the CM program provide procedures to identify and resolve issues necessary to enable or improve the CM posture of the organization, to include periodic vulnerability assessments, process improvements, technological advances, etc.?
14. Does the CM program provide for testing, training, and exercising the CM plan?
15. Does the CM program establish the Commander's intent for CM before, during, and after an event?
16. Are CM program requirements entered into the Planning, Programming, Budgeting and Execution (PPBE) System to link desired improvements to the budget building and execution processes?

17. Does the CM program provide the necessary HR support to staff the implementation and execution of the CM Plan?

18. Does the CM program consider command and support relationships with host (or tenant) organizations affecting CM?

19. Does the CM program consider command and support relationships with supporting organizations affecting CM?

20. Does the CM program consider command and support relationships with private sector organizations affecting CM?

21. Does the CM program include up-to-date agreements with host (or tenant) organizations (MOUs, ISSAs, etc.)?

22. Does the CM program include up-to-date agreements with supporting organizations (MOUs, ISSAs, etc.)?

23. Does the CM program include up-to-date agreements with private sector organizations (MOUs, ISSAs, etc.)?

24. Has the command published an integrated all-hazards CM/COOP plan [see Section B, below]?

25. Has the Commanding Officer signed the plan?

26. Did the local First Responders/Emergency Management Office/Host Command review the supportability of the plan?

27. Do Command actions demonstrate implementation of the CM/COOP plan?

SECTION B: CM PLAN

SUB-SECTION 1: *COMMAND AND CONTROL*

28. Does the plan identify, by billet, primary leadership and key personnel?

29. Does the plan identify primary contact information for primary leadership and key personnel?

30. Does the plan identify the primary leadership notional location during all event phases (Pre-event, Response, Recovery, and Reconstitution)?

31. Does the plan identify, by billet, alternate leadership and key personnel?

32. Does the plan identify the alternate leadership contact information?

33. Does the plan identify the alternate leadership notional location during all event phases (Pre-event, Response, Recovery, and Reconstitution)?

34. Does the plan include the use of the National Incident Management System (NIMS)?

35. Does the plan provide for the succession of leadership?

36. Does the plan designate the primary organic Response Team members?

37. Does the plan designate the alternate organic Response Team members?

38. Does the plan designate the augment EOC staff?

39. Does the plan designate the primary Watch teams?

40. Does the plan designate the alternate Watch teams?

41. Does the CM Plan ensure 12-hr restoration of continuity of leadership?

42. Does the CM Plan provide for a smooth transition from Response to Recovery without operational pause?

43. Does the CM Plan provide procedures to return the organization to normal operations (post-event)?

44. Does the plan identify a notional timeline of critical C2 events during execution? For example: Event (E) to E+1 Hr, E+1 to E+4 Hrs, E+4 to E+12 Hrs, E+12 to E+24 Hrs, E+24 to E+48 Hrs

45. Does the plan provide for executing the plan with Notice?

46. Does the plan provide established criteria for executing the plan without notice (No-Notice execution)?

47. Does the plan provide procedures to notify Higher HQ?

48. Does the plan identify a primary Emergency Operations Center (EOC) capable of managing the response and recovery of the event?

49. Is the EOC sufficiently separated from danger zones (i.e. building collapse zones) to reduce likelihood of destruction by same event?

50. Is the EOC prepared for immediate use?

51. Can the EOC immediately support Command and Control functions?

52. Can the EOC immediately support integrated communication functions?

53. Does the EOC immediately receive necessary logistical support?

54. Is the EOC coordinated with and mutually supportive of First Responders?

55. Does the plan identify an alternate EOC capable of managing the response and recovery of the event should the primary EOC be lost?

56. Does the plan provide standard operating procedures for the EOC?

57. Does the plan designate primary EOC personnel sufficient for 24/7 operations?

58. Does the plan designate alternate EOC personnel sufficient for 24/7 operations?

59. Does the plan include shelter activation procedures?

60. Does the plan provide communications between shelters and the EOC?

61. Does the plan provide a method (colored vests, badges, etc.) to identify key personnel?

62. Does the plan identify the process for command and control of ASF?

63. Does the plan designate the operational limitations of the ASF?

64. Does the plan coordinate ASF functions with organic, host, or local security forces?

65. Are alternate sites supporting continuity identified by directions (map)?

66. Are alternate sites supporting relocation of MEFs identified by directions (map)?

67. Are alternate sites supporting assumption of MEFs identified by directions (map)?

68. Does the plan detail command and control procedures to support movement to alternate sites?

69. Does the plan provide control procedures for the deliberate graceful degradation of MEFs?

SUB-SECTION 2: ***OPERATIONS***

70. Does the plan identify the MEFs?

71. Does the plan identify the priority of MEFs?

72. Does the plan identify the assets in direct support of MEFs?

73. Does the plan identify the associated processes that generate MEFs?

74. Does the plan identify the associated dependencies that generate MEFs?

75. Does the plan identify the associated relationships that generate MEFs?

76. Does the plan maintain sustained MEF operations for up to 30 days?

77. Does the plan identify procedures to relocate and/or reassign MEFs?

78. Does the plan identify procedures to recover MEFs in-place?

79. Does the plan identify back-ups for vital records to perform MEFs?

80. Does the plan identify back-ups of equipment to perform MEFs?

81. Does the plan identify factors equaling MEF disruption?

82. Are MEF disruptions defined in terms of time from disruption to adverse customer impact?

83. Are MEF disruptions defined in terms of recovery time estimates and objectives?

84. Does the plan identify a notional timeline of critical operational events during execution?
For example: Event (E) to E+1 Hr, E+1 to E+4 Hrs, E+4 to E+12 Hrs, E+12 to E+24 Hrs, E+24 to E+48 Hrs

85. Does the plan provide procedures to notify customers (those who use the products of the MEFs)?

86. Does the plan provide procedures to notify suppliers (those who provide input necessary to generate the MEFs)?

SUB-SECTION 3: ***HUMAN RESOURCES / PUBLIC RELATIONS / PUBLIC AFFAIRS:***

87. Does the plan identify critical MEF billets?

88. Does the plan identify key personnel?

89. Does the plan identify critical low-density skill sets (CLDS)?

90. Does the plan identify procedures to replace personnel?

91. Does the plan identify personnel requiring access to the facility during and after an event?

92. Does the plan identify organic personnel requiring access to the facility during and after an event?

93. Does the plan identify First Responders requiring access to the facility during and after an event?

94. Does the plan identify Repair/Recovery personnel requiring access to the facility during and after an event?

95. Does the plan identify support contractors requiring access to the facility during and after an event?

96. Does the plan identify service providers requiring access to the facility during and after an event?

97. Does the plan provide evacuation procedures for critical facilities?

98. Does the plan provide evacuation procedures for the installation?

99. Does the evacuation plan integrate with the local Emergency Management office for large-scale (mass) evacuation?

100. Does the plan provide procedures to shelter-in-place?

101. Does the plan include shelter access procedures?

102. Does the plan identify shelter supervisory personnel?

103. Does the plan designate muster sites for each facility?

104. Does the plan ensure muster sites have sufficient separation from danger areas (i.e.: building collapse zone)?

105. Does the plan designate alternate muster sites?

106. Are muster sites coordinated with First Responders?

107. Does the plan provide procedures for accountability musters?

108. Are there procedures to report accountability musters to the EOC?

109. Does the plan provide recall procedures?

110. Does the plan identify job-related HR counseling capabilities?

111. Does counseling include grief assistance?

112. Does counseling include legal assistance?

113. Does counseling include family assistance?

114. Does the plan provide a means to obtain public affairs support?

115. Does the plan designate locations for public relations briefs?

116. Does the plan provide standard 'emergency response' releases for various (most likely) events?

117. Does the plan provide standard pamphlets and read-ahead material available for media?

118. Does the plan provide procedures to provide access for media personnel?

119. Does the plan deconflict muster sites amongst facilities throughout the installation?

SUB-SECTION 4: ***SECURITY***

120. Is the EOC properly secured

121. Are MEF security requirements integrated with installation AT/FP Plan? (including Auxiliary Security Forces)

122. Does the plan identify security requirements for Mission Essential Functions?

123. Does the plan identify critical security billets specific to each MEF?

124. Does the plan provide a method to pass personnel on to or off of the facility?

125. Does the plan allow for rapid access to the installation? (First Responders, critical personnel, designated repairmen, etc)

126. Does the plan identify escort requirements?

127. Does the plan identify liaison requirements with local authorities?

128. Does the plan integrate internal and external security communications?

129. Does the plan consider jurisdictional boundaries?

130. Does the plan consider requirements for emergency destruction of classified material?

131. Does the plan consider requirements for emergency relocation of classified material?

132. Does the plan provide a timeline to de-brief First Responders after entrance to classified spaces?

133. Does the plan designate the location to debrief First Responders after entrance to classified spaces?

134. Is necessary documentation needed to de-brief First Responders after entrance to classified spaces identified?

135. Is there a method to coordinate with First Responders for de-briefing purposes after entrance to classified spaces?

136. Does the plan provide procedures to cordon off affected areas; allowing for normal operations in non-affected areas?

137. Does the plan address security requirements related to relocation?

SUB-SECTION 5: ***COMMUNICATIONS***

138. Does the plan identify primary communication methods?

139. Does the plan identify alternate communication methods?

140. Does the plan identify non-secure communications systems?

141. Does the plan identify secure communications systems, as required?

142. Are MEFs requirements integrated into the communications plan?

143. Are EOCs requirements integrated into the communications plan?

144. Are First Responders requirements integrated into the communications plan?

145. Are Local Emergency Shelters requirements integrated into the communications plan?

146. Are local supporting agencies' capabilities integrated into the communications plan?

147. Is the general organization (internal) requirements integrated into the communications plan?

148. Are customers requirements integrated into the communications plan?

149. Are suppliers requirements integrated into the communications plan?

150. Are host/tenant organizations requirements integrated into the communications plan?

151. Are higher HQ requirements integrated into the communications plan?

152. Does the plan identify critical MEF communications billets?

153. Does the plan identify primary telecom providers?

154. Does the plan identify alternate telecom providers?

155. Does the plan identify emergency communications equipment?

156. Does the plan provide procedures to issue emergency communications equipment?

157. Does the plan provide procedures to recover communications equipment?

158. Does the plan include the use of mass-notification systems, such as auto-notify, sirens, PA systems, etc.?

159. Does the plan include the use of alternate mass-notification systems?

160. Does the plan account for the installation's priority for restoration by telecom providers?

SUBSECTION 6: ***FACILITIES***

161. Are the EOCs properly sized to accomplish mission?

162. Does the plan designate the location of MEFs?

163. Does the plan identify critical MEF facility billets?

164. Does the plan designate the location of the EOC?

165. Does the plan designate the location of an alternate EOC?

166. Does the plan designate the location of in-place shelters?

167. Does the plan document the in-place shelter capacity?

168. Does the plan include procedures to obtain and update shelter certification?

169. Does the plan document supplies for in-place shelters?

170. Does the plan designate alternate sites for continuity?

171. Do alternate sites supporting continuity possess facilities to support organizational personnel?

172. Do continuity tests and exercises include alternate facility capabilities?

173. Does the plan designate alternate sites for relocation of MEFs?

174. Are alternate sites supporting relocation of MEFs documented in formal agreement?

175. Do alternate sites supporting relocation of MEFs possess facilities to support organizational personnel?

176. Are alternate sites supporting relocation of MEFs regularly tested as part of the plan?

177. Does the plan designate alternate sites capable of assuming MEFs?

178. Are alternate sites supporting assumption of MEFs documented in formal agreement?

179. Do alternate sites supporting assumption of MEFs possess facilities to support organizational personnel?

180. Does the plan identify facilities in support of the MEFs?

181. Does the plan identify security buildings and headquarters?

182. Does the plan identify staging areas?

183. Do facility evacuation plans direct people to designated muster areas?

184. Does the plan designate the location of up-to-date building plans and diagrams?

185. Does the plan provide an alternate location for building plans and diagrams?

186. Does the plan require cyclic updates of facility plans and diagrams to the EOC?

187. Does the plan provide facility access procedures to pass First Responders to unclassified spaces?

188. Does the plan provide facility access procedures to pass First Responders into classified spaces?

189. Do facility access procedures include the use of escorts?

190. Do facility access procedures include coordinating instructions, such as the location of access keys, etc.?

191. Are alternate sites supporting continuity documented in formal agreement?

SUB-SECTION 7: ***UTILITIES***

192. Does the plan identify primary utility providers?

193. Does the plan identify MEF electrical requirements?

194. Does the plan identify MEF fuels requirements, by type?

195. Does the plan identify MEF potable water requirements?

196. Does the plan identify MEF non-potable water requirements?

197. Does the plan identify emergency utility providers?

198. Does the plan identify the procedures to obtain and deploy emergency utilities?

199. Does the plan designate personnel to operate emergency utilities (and cut-off switches) for each disrupted facility?

200. Are alternate personnel identified to operate emergency utilities?

201. Does the plan account for the installation's priority for restoration by local utility providers?

202. Does the plan make use of organic utility capabilities?

203. Does the plan identify the priorities for deployment of emergency utilities?

SUB-SECTION 8: ***EQUIPMENT***

204. Are alternate sites supporting continuity sufficiently equipped to operate within 12 hours?

205. Are alternate sites supporting relocation of MEFs sufficiently equipped to operate within 12 hours?

206. Are alternate sites supporting assumption of MEFs sufficiently equipped to operate within 12 hours?

207. Does the plan identify MEF equipment requirements?

208. Does the plan identify critical MEF equipment operator billets?

209. Does the plan provide procedures to obtain replacement equipment?

210. Does the plan identify multiple sources of supply for replacement equipment?

211. Does the plan identify supplier POCs (24/7 ideal) for replacement equipment?

212. Does the plan detail requisition procedures for alternate equipment?

213. Does the plan identify order-to-delivery time requirements for replacement equipment?

214. Does the plan identify the locations of organic equipment suitable for use as replacements?

SUB-SECTION 9: ***TRANSPORTATION***

215. Does the plan identify MEF transportation requirements?

216. Does the plan identify critical MEF transportation coordination billets?

217. Does the plan address sources of transportation to support local evacuation

218. Does the plan address destination or release points to support local evacuation?

219. Does the plan address sources of transportation to support mass evacuation

220. Does the plan address destination or release points to support mass evacuation?

221. Does the plan address sources of transportation to support relocation?

222. Does the plan address escort requirements to support relocation?

223. Does the plan address primary and alternate routes to support relocation?

224. Does the plan address coordination with local and state movement control agencies to support relocation?

225. Does the plan address staging areas at origin and destinations to support relocation?

226. Does the plan address Material Handling Equipment requirements to support relocation?

227. Does the plan address transportation timelines to support relocation?

228. Does the plan address transportation timelines to support mass evacuation?

229. Does the plan address transportation timelines to support local evacuation?

230. Does the plan address Material Handling Equipment requirements to support mass evacuation?

231. Does the plan address Material Handling Equipment requirements to support local evacuation?

232. Does the plan address staging areas at origin and destinations to support mass evacuation?

233. Does the plan address staging areas at origin and destinations to support local evacuation?

234. Does the plan address coordination with local and state movement control agencies to support mass evacuation?

235. Does the plan address primary and alternate routes to support mass evacuation?

236. Does the plan address destination or release points to support relocation?

237. Does the plan address coordination with local and state movement control agencies to support local evacuation?

238. Does the plan address primary and alternate routes to support local evacuation?

SUB-SECTION 10: ***SERVICES***

239. Does the plan identify services required to directly sustain MEFs?

240. Does the plan identify services (i.e. food, house keeping, etc.) in general support of the installation?

241. Does the plan provide procedures to maintain services required to sustain MEFs?

242. Does the plan address procedures to replace each required service?

243. Does the plan address requirements for security clearances or badges for service provider?

244. Does the plan address the special knowledge, skills, and abilities required of any service providers?

245. Does the plan address timelines to replace each required service?

246. Does the plan provide procedures to pass key contractor personnel on to or off of facility?

247. Does the plan identify alternate sources of required services?

248. Does the plan identify specific services required for particular timephases of plan execution (i.e. portable latrines, kitchen services, etc)?

SUB-SECTION 11: ***IT/IS***

249. Does the plan identify the IT/IS data requirements to sustain MEFs?

250. Does the plan identify the IT/IS system requirements to sustain MEFs?

251. Does the plan identify the IT/IS program application requirements to sustain MEFs?

252. Does the plan identify critical MEF IT/IS billets?

253. Does the plan identify the vital records necessary to sustain MEFs?

254. Does the plan identify the databases necessary to sustain MEFs?

255. Does the plan sustain IT/IS capabilities in support of MEFs?

256. Does the plan specifically provide for the backup of critical data?

257. Does the plan specifically provide for the backup of critical systems?

258. Does the plan specifically provide for the backup of critical programs?

259. Does the plan specifically provide for the replication of systems architecture?

260. Does the plan capitalize on the IT Recovery Plan's Recovery Point Objectives?

261. Does the plan capitalize on the IT Recovery Plan's Recovery Time Objective?

262. Does the plan capitalize on the IT Recovery Plan's frequency of data back-up?

263. Does the plan identify the storage location for backed-up data, systems and programs?

264. Is the alternate location supporting IT backup sufficiently remote to preclude its loss during a disruptive event?

265. Does the plan provide procedures to restore IT capability to pre-event levels of access and utility or designated levels of degradation?

266. Is the alternate location supporting IT backup sufficiently accessible to organic personnel and designated external support personnel?

267. Is the alternate location supporting IT backup properly protected commensurate with the security level of the data?

268. Is the primary IT located appropriately to preclude its loss during a disruptive event?

269. Is the primary IT storage location supporting IT backup sufficiently accessible to organic personnel and designated external support personnel?

270. Is the primary IT storage location supporting IT backup properly protected commensurate with the security level of the data?

SUB-SECTION 12: *FINANCE, CONTRACTS, AND PURCHASING*

271. Does the plan identify a contracting agency and procedures to support MEFs?

272. Does the plan identify critical MEF fiscal billets (Finance, Contracting, or Purchasing)?

273. Does the plan provide fiscal procedures to support MEFs?

274. Does the plan include approval authority for various spending limits?

275. Does the plan include critical fiscal procedures?

276. Does the plan include record keeping?

277. Does the plan include reporting and audit requirements?

SUB-SECTION 13: ***ENVIRONMENTAL, HEALTH AND SAFETY***

278. Does the plan identify local military and civilian hospital capabilities and limitations?

279. Does the plan identify supporting Emergency Room facilities and capacities?

280. Does the plan identify supporting trauma facilities?

281. Does the plan identify supporting in-patient facilities?

282. Does the plan provide a response to Environmental, Health and Safety issues?

283. Does the plan designate evacuation assistants?

284. Does the plan designate evacuation floor monitors?

285. Does the plan provide a response to CBRNE issues impacting MEFs and installation?

286. Does the plan provide a response to HAZMAT issues impacting MEFs?

287. Is the plan supported by an integrated Mass Casualty Plan for the installation and local area?

SUB-SECTION 14: ***FIRST RESPONDERS***

288. Does the plan identify First Responder infrastructure? (Fire Stations, Police Stations, etc)

289. Does the plan integrate with First Responders?

290. Does the plan include the use of liaison officer(s) with First Responders?

291. Does the plan integrate with the First Responders' use of NIMS?

292. Does the plan coordinate MEF priorities to First Responders?

293. Does the plan provide First Responders with up-to-date building plans and diagrams?

294. Does the plan coordinate installation and First Responder footprint requirements?

295. Does the plan coordinate the location of the EOC with First Responders?

296. Does the plan coordinate the location of equipment staging areas with First Responders?

297. Does the plan coordinate the location of logistical support areas with First Responders?

298. Does the plan coordinate First Responder access control points?

299. Does the plan address procedures for Mass Casualty response?

300. Does the plan designate a triage site?

301. Does the plan designate a mass casualty site?

302. Does the plan designate a decontamination site?

303. Does the plan designate medivac helicopter landing zones?

304. Does the plan designate staging sites for medical evacuation?

305. Does the plan require periodic validation of requirements for mutual aid agreements with local First Responders?

SUB-SECTION 15: ***LEGAL***

306. Does the plan identify the provider and location of legal support services (organic or external)?

307. Does the plan designate the supporting staff Judge Advocate?

308. Does the plan consider legal liabilities and implications of installation events that affect the local surrounding area?

309. Does the plan meet the requirements for fiduciary responsibility?

APPENDIX D: PLANNING CONSIDERATIONS

Appendix D: Planning Considerations

This Appendix introduces building blocks for CM planners to consider when formulating plans. These building blocks are drawn from issues relevant to each of the four phases of CM, organized by those impacting the various CM teams, followed by those associated with each of the 15 functional areas. Experience suggests the issues addressed here bear consideration by CM planners, yet actions recommended are by no means all inclusive, nor applicable to all CM teams. The graphic below will assist the reader in understanding where they are in the three-dimensional matrix; additionally, the event phase and Team/MEF orientation will appear in the upper right margin of each page. Keep in mind that all issues are considered during the Pre-Event, or COOP planning phase, and are presented here in the context of the event phase in which they would be executed.

Pre-Event Phase	Response Phase	Recovery Phase	Reconstitution Phase
Team Issues	*Team Issues*	*Team Issues*	*Team Issues*
MEF Issues	*MEF Issues*	*MEF Issues*	*MEF Issues*

The intent is to provide functional area planners with a ready reference and resource to aid in the development of CM plans tailored to specific requirements using a deliberate, iterative process designed to ensure a fully integrated product. The planning team presents and addresses issues, concerns, and recommended planning factors to functional area experts as they influence MEFs. Although presented in the context of individual CM teams organized for each phase of a disruptive event, many if not most DON installations will of necessity rely on a less-robust CM organization. The planning considerations, by phase, remain the same regardless of the organizational matrix.

PRE-EVENT PHASE

PRE-EVENT TEAM ISSUES

The Pre-Event Team should function on a near-continuous basis, ensuring full-time integration of CM issues into the organization, and between functional areas. In practice, the CM Plan is never 'finished', as changes to the organization and its processes dictate the continuous evolution of continuity plans. Experience suggests several areas of consideration that Pre-Event planners may wish to review.

PRE-EVENT PHASE	RESPONSE PHASE	RECOVERY PHASE	RECONSTITUTION PHASE
TEAM ISSUES	TEAM ISSUES	TEAM ISSUES	TEAM ISSUES
MEF ISSUES	MEF ISSUES	MEF ISSUES	MEF ISSUES

Below are additional issues relating to the 15 identified functional areas, however they are by no means all-inclusive.

PRE-EVENT TEAM ISSUES

COMMAND AND CONTROL. ***HAVE YOU CONSIDERED:***

1. How establishing and maintaining leadership awareness of the CM environment assists the CM team to foster a 'mission assurance' culture within the organization?

2. Developing CM project management core competencies?

3. Authorization for Succession of Leadership and fiduciary positions within the CM Team organization?

4. Delegation of various authorities in the absence/loss of key leadership?

OPERATIONS. ***HAVE YOU CONSIDERED:***

1. A charter listing team responsibilities and actions?

2. All identified triggers that will cause activation of, or changes to, CM plans?

3. All actions to occur under various notional scenarios requiring plan activation, including actions under both notice and no-notice conditions?

4. The integration of the CM plan with internal and external customers, partners, and selected areas of the adjacent community?

5. A periodic validation of the plan to ensure its viability?

6. External partner awareness of changes to plans that they support?

7. Documentation of lessons learned during training and exercises to engender updates to the CM Plan?

8. The means of conveying essential plan information external to the organization?

9. The means to maintain currency of mutual aid agreements and other CM documents? Examples include:

    - Memoranda of Agreement/Understanding
    - Maps, blueprints and other graphics
    - Routes in and out of the location
    - Any negotiated contractual instruments supporting the agreements.

10. Existing disaster response plans such as fire, flood, chemical spill, hazardous materials, earthquake, etc?

HUMAN RESOURCES AND PUBLIC RELATIONS. ***HAVE YOU CONSIDERED:***

1. The composition of the Pre-Event Team, to include alternates?

2. Using the same people for the entire CM effort, from planning through development and execution of all 4 phases of the CM Plan?

3. Specific team composition during each CM phase?

4. Requirements to sustain 24x7 team operations?

5. The recall of CM team members?

6. A system of badges and/or colored apparel to organize, identify, and control the various responder teams (e.g. red vests for floor evacuation guides; blue vests for damage assessors)?

7. Requirements for security clearances and security access?

8. Public relations requirements?

9. A comprehensive media plan for circumstances where the nature of operations suggests potential high media interest?

COMMUNICATIONS. ***HAVE YOU CONSIDERED:***

1. A communications system to ensure continuous command and operation of the organization?

2. Primary and alternate communications procedures for internal CM team communication?

3. Communications interoperability with first responders?

4. A primary and alternate means of communication for leadership?

FACILITIES. ***HAVE YOU CONSIDERED:***

1. Facilities requirements for conducting CM Team activities across the spectrum of anticipated operations?

2. Steps to ensure back-up team facilities are not subject to the same effects that may render the primary team facility untenable?

3. Capacity and capability to sustain 24-hour team operations?

4. Uninterrupted power source requirements?

5. Temporary housing/health and comfort support?

6. Internal and external security of the team facility including access control, secure storage, secure meeting areas, ability to support secure communications?

7. Parking and logistics supportability/access, to include accommodation of potential media?

UTILITIES. ***HAVE YOU CONSIDERED:***

1. Utilities requirements at primary and alternate team sites? Factors to consider include:

    - Primary and alternate sources for team use during implementation and training exercises
    - Electrical Power
    - Potable water
    - Commercial communications
    - Battery requirements for back-up systems
    - Personal and industrial sanitation requirements
    - Fuel requirements (delivery to alternate site, storage, and safety)

EQUIPMENT. ***HAVE YOU CONSIDERED:***

1. Team equipment requirements for implementation, training and exercises? Issues include:

    - Communication devices (i.e. loudspeakers, bullhorns)
    - Visual Identifiers (i.e. vests, helmets, whistles)
    - Portable IT/IS equipment (i.e. laptop)

- Mobile EOC
- Mobile Electric Power
- Training Aids
- Audio Visual Equipment
- Barricades
- HAZMAT materials

TRANSPORTATION. ***HAVE YOU CONSIDERED:***

1. Dedicated or recurring transportation requirements to support Pre-Event CM operations in areas such as liaison trips, training, inspections and exercises?

SUPPORT SERVICES. ***HAVE YOU CONSIDERED***:

1. Services required to support Pre-Event CM team activities throughout planning, training, and exercises? Issues include:
    - Consultants
    - Plan Auditors
    - Exercise Management Support

IT/IS. ***HAVE YOU CONSIDERED:***

1. A plan to distribute IT equipment to team members required to support notice and no-notice execution of the CM plan?

2. Locating the equipment in protected areas accessible to team members?

3. A periodic evaluation to ensure equipment operability and team familiarity with its operation?

FISCAL. ***HAVE YOU CONSIDERED:***

1. The Fiscal requirements to support implementation, training and exercise of the plan? Specific issues include:
    - Budgeting for training exercises
    - Internal/external education and training
    - Attendance at conferences
    - Funding for training equipment

FIRST RESPONDERS. ***HAVE YOU CONSIDERED:***

1. Opportunities to increase the organizational knowledge base of the team as well as individual skills through

interaction with local first responders and State and Federal agencies?

2. Common language, equipment, and practices to increase the synergism of the team with external supporting agencies?

3. Engaging local first responders to conduct or participate in on-site surveys, inspections, training and exercises to help identify requirements in the Pre-Event phase?

LEGAL. ***HAVE YOU CONSIDERED:***

1. Ensuring the pre-event team is aware of the legal rules of the road when establishing CM plans and related activities?

PRE-EVENT PHASE MEF ISSUES

PRE-EVENT PHASE	RESPONSE PHASE	RECOVERY PHASE	RECONSTITUTION PHASE
TEAM ISSUES	TEAM ISSUES	TEAM ISSUES	TEAM ISSUES
MEF ISSUES	MEF ISSUES	MEF ISSUES	MEF ISSUES

CM Planners should consider the following issues, presented by functional area, for inclusion in their CM Plan.

FUNCTIONAL AREA ISSUES

COMMAND AND CONTROL. ***HAVE YOU CONSIDERED:***

1. How to employ and support an independently functioning Command Control system fully integrated with commercial entities and with civil authorities (federal, state and local)?

2. An Emergency Operations Center (EOC), to include the following issues?

   - Conditions and procedures for activation
   - Staffing requirements (including alternate staff members) to include liaison members for external agencies (e.g.: First Responder EOC)
   - Facility requirements
   - Communications capabilities necessary to support EOC operations
   - Coordination of ICS-related events
   - Notional list of staff responsibilities and daily schedule of events

3. Using an internal Incident Command System (ICS) to maintain situational awareness and coordinate actions in response to the event?

4. Which periodic reports to leadership will provide the status of the CM posture of organization and training?

5. How to incorporate leadership into the exercise plans?

6. How the command will consult with external agencies to include disaster relief, first responders, local government and contracted service providers?

7. Decision points requiring command action?

8. How the entire organization will be provided updates and information?

9. The succession of leadership and other positions within the organization?

10. How to delegate various authorities in the absence or loss of leadership positions?

OPERATIONS. ***HAVE YOU CONSIDERED:***

1. The operational characteristics in sufficient detail to facilitate the action during plan execution?

2. A prioritized list of MEFs and the impact of their loss on the mission?

3. The specific criteria and procedures required to execute the CM Plan, to include notice and no-notice implementation?

4. The concept of operations that supports the MEF during emergency operations?

5. Specific CM roles and responsibilities?

6. Identification of commercial dependencies?

7. Actions necessary to reduce or eliminate supply chain exposures?

8. How to integrate operational issues with internal and external customers, adjacent organizations and suppliers?

9. How the Plan will provide for notification of the leadership chain, customers and all third party suppliers and shippers of relocation to alternate sites?

10. How to integrate internal operation requirements with external local or municipal service providers?

11. How to document the location of Memoranda of Understanding and Agreement, Service Level Agreements, contracts and appropriate formal agreements with all concerned?

12. How to document and utilize action plans to address likely, realistic potential threats and events?

13. How to employ an enterprise-wide communications plan?

14. How the traffic management procedures to support emergency access and evacuation routes will impact operations?

15. Periodic tests and exercises of your recovery plan?

16. Detailed face-to-face planning and coordination with all supporting resources and service providers?

17. The extent to which elements within the organization rely on Supervisory Control and Data Acquisition (SCADA) and Process Control Systems for automated control?

HUMAN RESOURCES AND PUBLIC RELATIONS. ***HAVE YOU CONSIDERED:***

1. The internal and external people requirements of each MEF?

2. How the loss of people will impact the MEF?

3. Mission essential personnel requirements for each MEF-related action, to include recall data for primary and alternate personnel? Refer to Tables C-1 and C-2.

4. Whether MEF support people including alternates have proper security clearances?

5. The procedures to account for all people in the event of evacuation?

6. The procedures people will use to execute the plan?

I. PEOPLE CONTACT REQUIREMENTS	PRE-EVENT
Communications Support People	
Contracting Authorities	—X—
Counselors - Personal and Religious	
Supported Unit - Reliant on MEF	—X—
Facilities - Owner, Landlord, Management	
Alternate Facility Managers	—X—
IT/IS Support People	—X—
Local Emergency Responders	—X—
Mission Essential and Augment People	—X—
Security Points of Contact	—X—
Government Service Providers	—X—
Services - Critical Service/Services Providers	—X—
Services - Critical Services Operations People	—X—
Suppliers	—X—
Team Members	—X—
Transportation Service Providers	—X—
Utility Support Providers	—X—

TABLE C-1. PEOPLE CONTACT COORDINATION TABLE

7. The training requirements for all key people likely to initiate plan execution?

8. Any media points of contact?

9. The additional manpower/sourcing requirements to support the implementation and execution of the plan?

10. The potential public interest implications for organization?

11. The implications that implementation or execution will have on supported activities?

12. Letters assigning individuals to various CM positions with the organization?

SECTION 1.02	
Organization Name	
Contact Name	
Address	
Phone	
Cell Phone	
Pager	
Personal Digital Assistant (PDA)	
e-Mail	
Website/URL	

TABLE C-2. RECALL TABLE

SECURITY. ***HAVE YOU CONSIDERED:***

1. The internal and external security requirements of each MEF?

2. How the loss or degradation of security capability will impact MEFs?

3. How to meet the heightened security requirements likely required during an event?

4. Security requirements and procedures for classified material, to include primary and alternate sites?

5. Security of funds, contracts and fiscal requirements?

6. The appropriate level of clearance for the people necessary to implement and execute the Plan, to include primary and alternates, whether sourced from internal and external resources?

7. Procedures to debrief all un-cleared people (internal and external) involved in response and recovery operations?

8. Coordination issues with local authorities for the use of deadly force, if applicable?

9. The physical security issues with local security agencies?

10. How to coordinate the actions during a facility lockdown, including access procedures for essential people, first responders, or critical service repair people?

11. Points of contact for essential vendor and services people?

12. The identification and integration of jurisdictional boundaries with local, state, and Federal agencies?

13. The identification and integration of security actions for any local, state, or other Federal property located within the organization's jurisdiction?

14. A method to identify all response and recovery team people, to include badging, identification vests, etc.?

COMMUNICATIONS. ***HAVE YOU CONSIDERED:***

1. A communications plan to support pre-event training exercises?

2. The procedures to distribute communications equipment to appropriate people?

3. The communications characteristics (internal, external and contractor), secure and unsecured, necessary to support each MEF, to include the following?

    - Radio
    - Telephone
    - Cell Phone
    - Satellite communications
    - Data transmission
    - Internet
    - Fiber Optic
    - Infrared
    - Laser
    - Cable

4. How a loss or degradation of communications capability might impact MEFs?

5. The requirement for mass-notification procedures in support of both notice- and no-notice execution of the CM Plan?

6. At what point organization requires redundant communications capabilities?

7. Identifying primary and alternative sources (suppliers) for compatible communications equipment?

8. Communications equipment sourcing requirements?

FACILITIES. ***HAVE YOU CONSIDERED:***

1. The internal and external facilities characteristics that support MEFs?

2. How the loss or degradation of facilities will impact MEFs?

3. The location of and access to detailed (architectural) building plans for facilities housing or supporting MEFs?

4. Other elements of the business that may have facilities suitable for supporting MEFs?

5. The procedures to obtain, outfit, or relocate to alternate facilities in support of MEFs?

6. The nature of anticipated threats in determining locations for an alternate facility?

UTILITIES. ***HAVE YOU CONSIDERED:***

1. The internal and external utilities requirements of the MEFs?

2. How a loss or degradation of utilities will impact MEFs, to include the following?

    - Electrical power
    - Water
    - Communications links
    - Telephone (installed, cellular, and satellite)
    - Gas (LP or CNG)
    - Fuel

3. Recall data for utility support providers? Refer to People – Recall Data, Table III-2 for applicable contact data.

4. Identifying critical utility requirements to local utility providers, to include any applicable alternates?

5. Utility recovery/replacement criteria and processes?

6. Service Level Agreements with primary and alternate utility providers?

7. Alternative (redundant and/or independent) utility sources to sustain the MEFs?

8. Requirements for an uninterrupted power source?

OPERATIONAL EQUIPMENT. ***HAVE YOU CONSIDERED:***

1. The internal and external equipment requirements of each MEF?

2. How a loss or degradation of operational equipment will impact support to MEFs?

3. How to access the equipment necessary to support MEFs?

4. Equipment support requirements such as people to augment surge operations, maintenance and contractors, etc.?

5. Procedures to obtain and use training equipment?

TRANSPORTATION. ***HAVE YOU CONSIDERED:***

1. The internal and external transportation characteristics of each MEF?

2. How a loss or degradation of transportation capability will impact support to MEFs?

3. Training and exercise transportation requirements and capabilities?

4. Requirements and procedures to augment or recover equipment, services.

5. Routes and local Department of Transportation authorities required to move on various roads?

6. Procedures to support movement to an alternate location, to include the following?

    - Primary and alternate assembly area(s) for people and cargo?
    - Primary and alternate staging area(s) for people and cargo?
    - Primary and alternate routes to alternate locations.
    - Coordination requirements for movement control agencies (local or state DOT, etc.).
    - Identifying and coordinating alternate means of transport.

7. Coordinating emergency access and evacuation requirements (primary and alternate) with civil authorities (local, state and Federal)?

8. Recall procedures for transportation service providers and coordinators necessary to sustain the MEF? Refer to People – Recall Data, Table III-2 for applicable contact data.

SUPPORT SERVICES. ***HAVE YOU CONSIDERED:***

1. Prioritization of internal and external support services requirements of each MEF?

2. How a loss or degradation of support services will impact support to MEFs?

3. Identifying the procedures to obtain services?

4. Training and exercise support service requirements?

5. Coordinating with local, state and Federal emergency and relief service providers?

6. Access procedures for service people (EMS, law enforcement, contractors, etc.) to support MEFs during site lockdown?

7. Contact procedures for essential service providers who support MEFs? Refer to People – Recall Data, Table III-2 for applicable contact data.

(IT/IS). ***HAVE YOU CONSIDERED:***

1. The internal and external IT/IS characteristics of each MEF to include the following:
    - Technical and operational characteristics
    - Identifying critical data and files to include RTO/RPO for each
    - Critical hardware, software and operating systems
    - Alternate site for data center and/or network operation centers
    - Operators and technicians
2. How a loss or degradation of IT/IS services will impact support to MEFs?

3. Criteria and processes to recover or replace IT/IS services?

4. At least one alternate source of IT/IS service providers to support MEFs?

5. Primary and alternate suppliers for IT/IS Hardware, Software and peripherals?

6. Recall for IT/IS support and contractor people? Refer to People – Recall Data, Table III-2 for applicable contact data.

7. The location of current IT/IS system documentation, and the location of backup software, data, equipment inventories and assignments for use in developing equipment requirements to support recovery operations?

8. Testing and rehearsing IT/IS recovery capabilities regularly, to include the following?
    - Evaluate test and debrief participants,
    - Adjust IT/IS Recovery capabilities accordingly

FISCAL, CONTRACTING, AND PURCHASING. ***HAVE YOU CONSIDERED:***

1. The Fiscal, Contracting, and Purchasing requirements of each MEF, to include operational, maintenance, and replacement?

2. How a loss or degradation of Fiscal, Contracting, and Purchasing activities will impact support to MEFs?

3. The criteria and processes to recover or replace Fiscal, Contracting, and Purchasing services?

5. Modifications to contracts to allow non-prejudicial temporary modification to contract deliverables (stop, increase, decrease) during incident response, if possible?

6. CM fiscal, contracting and purchasing requirements funds for both Pre-Event training and exercises, and actual events, to include the following?

    - Permanent and/or temporary staff increases associated with the CM program
    - Training
    - Contingency contracts
    - Contingency procurements
    - CM exercises.
    - Procedures to capture contingency costs

7. Security of funds, contracts, and fiscal documents?

8. A primary and alternate contracting authority able to meet contract requirements in support of the CM effort? Refer to People – Recall Data, Table III-2 for applicable contact data.

ENVIRONMENTAL, HEALTH AND SAFETY. ***HAVE YOU CONSIDERED:***

1. The internal and external Environmental, Health and Safety requirements of each MEF?

2. Coordinating your requirements with external (non-resident) Environmental, Health and Safety providers?

3. How a loss or degradation of Environmental, Health and Safety conditions will impact support to MEFs?

4. Criteria and processes to recover or replace Environmental, Health and Safety services?

5. Points of contact, organic and external, for essential Environmental, Health and Safety services people?

6. Any environmental, health and safety related agreements with corresponding federal, state and local agencies?

7. All applicable Environmental, Health and Safety laws, regulations and requirements?

8. A regulatory compliance review of your CM program by Environmental, Health and Safety agencies?

9. Environmental, Health and Safety participation in training and exercises to support your CM plan?

10. Support for Environmental, Health and Safety access to all MEF-related facilities, installations and sites, to include access during lockdown?

11. A method to identify Environmental, Health and Safety services provider people such as access badges or vests?

12. As applicable, the following?
    - Isolation procedures and sites
    - Decontamination procedures and sites
    - Disposal process for contaminated material
    - Process to prevent cross contamination
    - Triage sites
    - Medical-evacuation sites
    - Alternate buildings or facilities where Environmental, Health and Safety activities could take place

FIRST RESPONDERS. ***HAVE YOU CONSIDERED:***

1. The method and magnitude of first responder presence at the installation?

2. The coordination of your CM actions with first responders such as the following?
    - Prioritized critical assets
    - Staging areas
    - Emergency routes
    - ICS
    - EOC
    - Aircraft landing zones

3. Mutual aid issues?

4. First responder participation in exercises, drills and rehearsals?

5. Attending off-site training and education sponsored by first responders?

LEGAL. ***HAVE YOU CONSIDERED:***

1. Installation-specific liability issues involved in contingency planning, stressing the strategic, moral, and legal obligations borne by the command?

2. Including contract clauses that provide for non-prejudicial temporary modifications to deliverables (stop, increase, decrease) during incident response?

3. Legal representation to advise during development of training and exercises?

4. Continuous access to legal records and files, including insurance, Human Resources and contracts-related documents?

RESPONSE PHASE

The purpose of Response phase planning is to coordinate initial on-scene emergency efforts and assist first responders who may be unfamiliar with the organization's assets and mission. The Response phase is perhaps the most difficult phase to plan. Particularly since Recovery actions may begin during the Response phase.
The intent of Response phase planning is for people to:

- Rapidly assess the disruptive event and implement knowledge based actions, similar to Emergency Medical Services during the "golden hour" following a traumatic event.
- Preserve the tempo of operations until a more definitive assessment of conditions permit detailed planning and actions.

RESPONSE PHASE TEAM ISSUES

PRE-EVENT PHASE	**RESPONSE PHASE**	RECOVERY PHASE	RECONSTITUTION PHASE
TEAM ISSUES	**TEAM ISSUES**	TEAM ISSUES	TEAM ISSUES
MEF ISSUES	MEF ISSUES	MEF ISSUES	MEF ISSUES

CM planners should develop the points provided under each of the functional areas, while focusing on the MEF's specific environment. This planning will provide the response team with a knowledge base to:

- Familiarize the response team with the MEF.
- Enable the response team to fully support the efforts of the First Responders.
- Identify and acquire the necessary equipment.
- Assess any damage or operational limitations.
- Provide the proper information to the command, and to Recovery Teams.
- Facilitate the timely start of Recovery phase.

FUNCTIONAL AREA ISSUES

COMMAND AND CONTROL. ***HAVE YOU CONSIDERED:***

1. The interoperability requirements for communicating with First Responders?

2. The responsibilities and role of the Response Team including reporting requirements?

3. Existing Response and Evacuation plans as appropriate?

4. Provisions to test and rehearse response procedures regularly, to include evaluating, testing, and debriefing Response Team members and participants, and adjusting the Response Plans accordingly?

5. The detailed characteristics and capabilities of each MEF?

6. Considered that the Response Team should develop the response phase of the CM plan?

7. Procedures to assess and report the effectiveness of the CM Plan to the CM Team?

8. Coordination of Response Team actions in support of both the organization (e.g.: Comannder's staff) and external support providers (e.g.: First Responders)?

9. Ensuring the easy identification of the team (access badges, colored jersey scheme, etc.) to all site management, security and law enforcement authorities?

10. Requirements for operating 24 hours a day, 7 days a week?

11. Post-event after action reports, debriefings, CM Plan revisions, etc.?

OPERATIONS. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of any loss or degradation to MEFs?

HUMAN RESOURCES AND PUBLIC RELATIONS. ***HAVE YOU CONSIDERED:***

1. Recall procedures for key people, including alternates?

2. Team training requirements, including damage assessment training and training in assessing impact to business processes?

3. Existing response and evacuation procedures as appropriate?

SECURITY. ***HAVE YOU CONSIDERED:***

1. Team member access to all MEF related facilities, installations and sites to include access while the facility is operating under restricted access?

2. Security requirements for Team members?

COMMUNICATIONS. ***HAVE YOU CONSIDERED:***

1. The interoperability requirements for communicating with First Responders?

2. The communications capabilities needed to support the Team, to include intra-team, internal, and external requirements?

3. Communications equipment to include mobile radios, crowd control, loud-speakers/bull horns, whistles, etc?

FACILITIES. ***HAVE YOU CONSIDERED:***

1. How you will meet the facilities requirements of operating 24 hours a day 7 days a week?

2. Requirements to support EOC operations, management or media briefing area, staging areas, muster/briefing area, access control point(s), etc?

3. Alternate facilities to support the Team?

4. The impact the location and mobility of the Team facility will have on their performance?

UTILITIES. ***HAVE YOU CONSIDERED:***

1. Utility support to the Team, to include mobile power?

2. Alternate utility support to the Team?

OPERATIONAL EQUIPMENT. ***HAVE YOU CONSIDERED:***

1. The equipment needs of the Response Team, to include specialized equipment?

2. The availability of maps, blueprints, HAZMAT supplies, mobile IT/IS systems, etc.?

TRANSPORTATION. ***HAVE YOU CONSIDERED:***

1. The transportation requirements of the Team?

2. Sourcing transportation support for the Team, to include any surge requirements?

SUPPORT SERVICES. ***HAVE YOU CONSIDERED:***

1. Internal and external service requirements necessary to sustain the Team such as power, telecommunications, food, fuel, sanitation, temporary lodging, etc.?

IT/IS. ***HAVE YOU CONSIDERED:***

1. IT/IS support to the Team, to include any mobile IT/IS assets?

2. The compatibility of Team IT/IS systems with other systems, to include First Responders?

FINANCE, CONTRACTS, AND PURCHASING. ***HAVE YOU CONSIDERED:***

1. How you will support the fiscal requirements of the Response Team?

2. How to support any surge requirements of the Team?

ENVIRONMENTAL, HEALTH AND SAFETY. ***HAVE YOU CONSIDERED:***

1. Environmental, Health and Safety related equipment to support the team?

2. How Environmental, Health and Safety will impact Team operations?

FIRST RESPONDERS. ***HAVE YOU CONSIDERED:***

1. The interoperability requirements for communicating with First Responders?

2. Initial information and coordination with First Responder to facilitate their actions?

3. Coordinating the initial on-scene linkup between the Team and the First Responder Incident Commander to facilitate a faster development of First Responder situational awareness?

4. The aspects, sequencing and timing to regain post-event control of the organizational areas or assets from the First Responder Incident Commander?

LEGAL. ***HAVE YOU CONSIDERED:***

1. Legal restrictions or requirements that impact the Team?

RESPONSE PHASE MEF ISSUES

Pre-Event Phase	**Response Phase**	Recovery Phase	Reconstitution Phase
Team Issues	Team Issues	Team Issues	Team Issues
MEF Issues	**MEF Issues**	MEF Issues	MEF Issues

FUNCTIONAL AREA ISSUES

COMMAND AND CONTROL. ***HAVE YOU CONSIDERED:***

1. Notice- and no-notice triggers to execute the plan?
2. Methods to concurrently manage both the event and maintain ongoing operations?
3. Criteria and procedures for emergency shutdown of elements of the organization?
4. Criteria and procedures for relocation of organizational functions?
5. Circumstances and procedures to conduct shelter in place?
6. Procedures to gain and maintain situational awareness during the event?
7. Informing all personnel, higher and adjacent organizations, and the public as to the nature of the event?
8. Criteria for triggers for activation of an Emergency Operations Center?
9. Internal emergency responses that require coordination with civil authorities, such as service providers, shelters, hospitals and alternate sites?
10. Maps, plans, diagrams, inventories, and documentation, software media and data that support MEFs?

OPERATIONS. ***HAVE YOU CONSIDERED:***

1. How the loss or degradation of operational function and capabilities will impact responding to MEF issues?
2. The priority of effort to maintain MEFs?
3. Emergency procedures to curtail or shut down operations?
4. Procedures to notify supporting and supported organizations?
5. Continuing limited operations?
6. Criteria and procedures for activating alternate site(s)?
7. The extent to which Supervisory Control and Data Acquisition (SCADA) and Process Control Systems manage areas within the organization?

HUMAN RESOURCES AND PUBLIC RELATIONS. ***HAVE YOU CONSIDERED:***

1. Procedures to maintain support of MEFs, given the loss of skilled operational staff members?

2. Contact data for local responders (medical facilities, fire, HAZMAT and law enforcement agencies servicing the local area?

3. How Human Resource Managers will access personnel records?

4. Requirements for alternate skilled staff to fill key positions?

5. How an event will impact the immediate and near term requirement to recall, augment or release personnel from duty?

6. Evacuation plans for each MEF related installation, to include the following?

    - Primary and Alternate Evacuation Routes
    - Primary and Alternate Assembly Areas,

7. How and when you will inform the media?

8. Provisions to obtain Counseling Services (Benefits, Religious, Legal, etc?)

9. Procedures for emergency contact notification in the event of casualties?

10. The priority of effort to maintain MEFs within Human Resources and Public Relations?

11. Procedures to account for all personnel including members of the staff, contractors, and visitors?

12. Security of personal and classified information and records?

SECURITY. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of any loss or degradation of security function on the MEF?

2. Security requirements in support of response actions for each MEF, to include the following?

    - Physical Security requirements,
    - Security of classified material, information, communications and equipment
    - The use of internal personnel to augment the security force to perform auxiliary functions such as watching over person and organizational property, directing the curious to security, etc.
    - Establishing traffic and access control.

3. The requirements to coordinate jurisdictional boundaries for security with adjacent municipalities and civil authorities (federal, state and local)?

4. Security requirements and procedures for evacuation of personnel and assets, to include the following?
    - Evacuees
    - Cleared staff to support operations at an alternate site.
    - Evacuating classified material and equipment

5. Emergency destruction requirements and procedures as appropriate?

6. The coordination of internal and external security forces with local/state/federal security officials?

7. Security clearance requirements for Response Team and emergency responders, whether internally or externally sourced?

8. Procedures to safeguard organizational and personal property, documents and other critical assets from looters, vandals, and others?

9. The priority of effort to maintain MEFs within Operations?

COMMUNICATIONS. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of communications capabilities on the support to MEFs?

2. A capability and alternate which provide interoperable communications with internal and external users including?
    - Staff
    - External responders
    - Internal responders
    - Supported, supporting and adjacent organizations

3. Communications support necessary to implement the Incident Command System (ICS)?

4. Appropriate security of classified communications equipment, data, material and assets?

5. The recall of communication support people associated with each MEF? Refer to Human Resources – Consequence Management, Table III- 2 for applicable contact data.

6. Periodic testing and rehearsing communications capabilities?

7. The priority of effort to maintain MEFs within security?

8. Procedures to expeditiously issue equipment while maintaining accountability?

FACILITIES. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of facilities on the ability to support the MEF?

2. The priority of effort to maintain MEFs within facilities?

3. Facility security requirements as they affect response actions, maintain physical security, safeguard classified material, assets, equipment, and secure communications?

4. Blueprints and architectural drawings of each facility for use by the response team?

5. Informing response personnel of the layout, location and function of critical facility features supporting the MEF, such as the following?

    - Windows,
    - Doors,
    - Ladders,
    - Stairwells,
    - Elevators,
    - Electrical panels,
    - Gas valves,
    - Water valves,
    - Fire alarm panels or systems,
    - Roads
    - Bridges
    - Access points.

6. Requirements for temporary facilities for such functions as the following?

    - Emergency operations
    - Unit operations
    - Staff
    - Health and comfort

7. Building management in leased facilities?

8. Other potential impacts of leased facilities?

9. Facility emergency shutdown?

UTILITIES. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of utilities on the ability to support the MEF?
2. Availability of utility systems installation drawings and manuals that display critical features supporting the MEF?
3. The impact of sudden loss of utilities on systems and equipment?
4. The locations of and procedures for emergency cut-off?
5. The recall and/or contact of key utility service providers supporting each MEF? Refer to Human Resources – Consequence Management, Table III-2 for applicable contact data.
6. Requirements for employing emergency utilities?
7. The priority of effort to maintain MEFs within utilities?
8. The extent to which Supervisory Control and Data Acquisition (SCADA) and Process Control Systems manages utilities?

OPERATIONAL EQUIPMENT. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of Operational Equipment on the ability to support the MEF?
2. Alternate sources of equipment to sustain MEFs?
3. MOUs or other applicable agreements to obtain short-duration replacement/augmentation equipment to support each MEF?
4. The need for additional Operational Equipment requirements and capabilities?
5. The priority of effort to maintain MEFs within Operational Equipment?

TRANSPORTATION. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of Transportation capability on the ability to support the MEF?
2. Surge transportation requirements necessary to support emergency response and unit operations such as the following?

- Security personnel,
- Classified Documents and equipment,
- Evacuation of local population,
- Movement of mass casualties to local supporting medical facilities

3. Primary and alternate routes to and from key infrastructure and coordinated/deconflicted routes with first responders and other authorities?

4. Requirements and/or sources for any special-use rolling stock and emergency vehicles?

5. Requirements for mobile command centers, internal security forces or first responders?

6. The priority of effort to maintain MEFs within Transportation?

SUPPORT SERVICES. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of Support Services on the ability to support the MEF?

2. Internal and external service requirements necessary to sustain each MEF such as power, telecommunications, food, fuel, sanitation, temporary lodging, etc.?

3. Contact data for Service providers associated with each MEF?

5. Sources to support operations 24 hours a day 7 days a week?

6. The priority of effort to maintain MEFs within Support Services?

IT/IS. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of IT/IS capabilities on the ability to support the MEF?

2. The security of classified IT/IS material and assets?

3. The recall or contact of IT/IS support staff associated with each MEF? Refer to Human Resources – Consequence Management, Table III-2 for applicable contact data.

4. The priority of effort to maintain MEFs within operations?

5. The extent dependencies upon Supervisory Control and Data Acquisition (SCADA) and Process Control Systems?

FISCAL, CONTRACTING, AND PURCHASING. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of Fiscal, Contracting, and Purchasing capabilities on the ability to support the MEF?
2. Fiscal and contracting guidance and authority to support the response effort?
3. Emergency contracting mechanisms to support each MEF?
4. Budget and funding requirements to staff, train and equip the Response team?
5. Procedures to obtain sufficient funds to support response operations?
6. Regulations and procedures to capture your costs of response operations?
7. Fiscal and contractual requirements to support emergency shutdown of business operations?
8. The priority of effort to maintain MEFs within Fiscal, Contracting and Purchasing?

ENVIRONMENTAL, HEALTH AND SAFETY. ***HAVE YOU CONSIDERED:***

1. Procedures to assess and report the impact of loss or degradation of Environmental, Health and Safety capabilities on the ability to support the MEF?
2. A primary and alternate authority to address Environmental, Health and Safety requirements?
3. Environmental, Health and Safety mechanisms to support each MEF?
4. The recall and or contact of Environmental, Health and Safety personnel?
5. Sourcing of equipment, communications, facility, transportation, detection devices, protective equipment and kits, and decontamination material required to support Environmental, Health and Safety requirements?
6. Environmental, Health and Safety regulations, implications and procedures for emergency shutdown of operations?
7. The priority of effort to maintain MEFs within Environmental, Health and Safety?
8. Procedures to determine hazards (WMD, HAZMAT, etc), including the following?
    - Identify means to counter and/or react to hazards,
    - Identify clean-up and disposal methods.
9. Emergency procedures to curtail or shut down operations?

FIRST RESPONDERS. ***HAVE YOU CONSIDERED:***

1. First Responder knowledge and familiarity with MEF characteristics?
2. How First Responders will gain access to base facilities during lockdown and non-business hours?
3. The recall of any organic first responders particular to each MEF?
4. Interoperable communications with First Responders, in particular with their EOC?
5. The priority of effort to maintain MEFs within First Responders?
6. How you will grant First Responders access to secure, sensitive and restricted areas?
7. The requirement to debrief First Responders after their entrance to sensitive or secure areas?
8. The requirement for escorts?
9. A full accountability of organization and First Responder property prior to the departure of First Responders?
10. A situation brief for First Responders upon their arrival?

LEGAL. ***HAVE YOU CONSIDERED:***

1. Security of access to personal and classified information and records?
2. The privacy of information for injured, missing, or deceased members of the organization?
3. The release of information to the public, media, customers, suppliers, and members of the organization?
4. The legal implications of emergency shutdown?
5. Personal and government liability issues?
6. The priority of effort to maintain MEFs within Legal?

RECOVERY PHASE

The purpose of the Recovery phase is to restore the minimal functionality to MEFs as quickly as possible. The Recovery phase provides the methodology for detailed damage assessment, recovery action plan validation or adjustment, and decision analysis and execution. Additionally, it provides a means of recommending various pre-planned courses of action from repair, replacement, or relocation of the MEFs to another facility in the shortest time. The effectiveness of the actions taken during the recovery phase will be essential to the organization's ability to survive a disruptive event.

RECOVERY PHASE TEAM ISSUES

Pre-Event Phase	Response Phase	**Recovery Phase**	Reconstitution Phase
Team Issues	Team Issues	**Team Issues**	Team Issues
MEF Issues	MEF Issues	MEF Issues	MEF Issues

The Recovery Team receives information from the Response Team, assesses any damage or operational limitations and effectively activates and directs the effort to recover operations. The Recovery Team also provides critical information to Emergency Operations Center that support leadership's actions to fully recover operations and prepare for the Reconstitution phase. Note that the Recovery Team integrates its efforts toward MEF recovery with those of the other plans and teams in each of the phases including internal and external support providers. The quick decisive actions of the Recovery Team enable the organization to continue its MEFs throughout the disruptive event.

Members of the Recovery Team should develop the action plans that support the Recovery phase in order to ensure complete familiarity with the actions it contains. In so doing, the Recovery Team must consider the requirements and qualification of those people assigned actions during the Recovery Phase.

FUNCTIONAL AREA ISSUES

MANAGEMENT AND CONTROL. ***HAVE YOU CONSIDERED:***

1. Requirements for operating 24 hours a day, 7 days a week?
2. The means to gain and maintain situational awareness?
3. The tools and information necessary to exercise the Teams' responsibilities?
4. The information flow between the Team and the command?
5. The tools and information that are required to make critical decisions as the recovery phase unfolds?
6. Flexibility to adapt to situations as they arise?
7. Which recovery decisions leadership will retain at their level?
8. The process to keep the Command informed?
9. Post-event after action reports, debriefings, CM Plan revisions, etc.?

OPERATIONS. ***HAVE YOU CONSIDERED:***

1. Operational characteristics and requirements of each MEF?

2. Maps, plans, diagrams, software, documentation and electronic media necessary to recover MEFs?

HUMAN RESOURCES AND PUBLIC RELATIONS. ***HAVE YOU CONSIDERED:***

1. The Teams' knowledge, expertise, and familiarity with recovering MEFs?

2. Recall data for Recovery Team members?

3. Specific training requirements for each MEF?

4. Procedures to identify the Team (access badges, colored jersey scheme, etc.) to internal and external security and law enforcement authorities?

SECURITY. ***HAVE YOU CONSIDERED:***

1. The security characteristics and requirements of each MEF, such as the sort/type of material held, clearances and "need-to-know" for access, and who are the primary and alternate custodians?

2. Appropriate security clearances, if required, to respond to each MEF?

3. The impact of introducing new or different classified material, equipment, software or processes to the recovery team as part of recovery?

4. The need for security escorts?

5. The requirements for recovery team access to the site(s) affected by the event?

6. The requirements for positive control of recovery team access to various locations, to include locations of people, badging, etc.

COMMUNICATIONS. ***HAVE YOU CONSIDERED:***

1. The Team's knowledge of communications properties, capabilities and requirements for each MEF?

2. The Team's capability to communicate with other CM Teams as well as other parties?

FACILITIES. ***HAVE YOU CONSIDERED:***

1. The facilities characteristics and capabilities of each MEF?

2. How you will meet the facilities requirements of operating 24 hours a day 7 days a week?

3. Requirements to support EOC operations, management or media briefing area, staging areas, muster/briefing area, access control point(s), etc?

4. Alternate facilities to support the Team?

5. The impact the location and mobility of the Team facility will have on their performance?

UTILITIES. ***HAVE YOU CONSIDERED:***

1. Utility support to the Team, to include mobile power?

2. Alternate utility support to the Team?

3. The Team's understanding of utilities' specifications and requirements for each MEF?

4. The Team's priority for utility recovery at both primary and alternate sites?

OPERATIONAL EQUIPMENT ***HAVE YOU CONSIDERED:***

1. The required documents, tools and repair parts to rapidly institute recovery?

2. The equipment needs of the Response Team, to include specialized equipment?

3. The availability of maps, blueprints, HAZMAT supplies, mobile IT/IS systems, etc.?

4. The Team's understanding of the equipment specifications, capabilities and requirements for each MEF?

TRANSPORTATION. ***HAVE YOU CONSIDERED:***

1. The transportation requirements of the Team?

2. Sourcing transportation support for the Team, to include any surge requirements?

SUPPORT SERVICES. ***HAVE YOU CONSIDERED:***

1. Internal and external service requirements necessary to sustain the Team such as power, telecommunications, food, fuel, sanitation, temporary lodging, etc.?

IT/IS. ***HAVE YOU CONSIDERED:***

1. IT/IS support to the Team, to include any mobile IT/IS assets?

2. The compatibility of Team IT/IS systems with other systems, to include First Responders?

3. The Team's understanding of the IT/IS characteristics, capabilities and requirements for each MEF.

FINANCE, CONTRACTS, AND PURCHASING. ***HAVE YOU CONSIDERED:***

1. Support for the Team?

2. How to support any surge requirements of the Team?

ENVIRONMENTAL, HEALTH AND SAFETY. ***HAVE YOU CONSIDERED:***

1. Environmental, Health and Safety related equipment to support the team?

2. How Environmental, Health and Safety will impact Team operations?

FIRST RESPONDERS. ***HAVE YOU CONSIDERED:***

1. The interoperability requirements for communicating with First Responders?

2. Initial information and coordination with First Responder to facilitate their actions?

3. Coordinating the initial on-scene linkup between the Team and the First Responder Incident Commander to facilitate a faster development of First Responder situational awareness?

4. The aspects, sequencing and timing to regain post-event control of organizational facilities from the First Responder Incident Commander?

LEGAL. ***HAVE YOU CONSIDERED:***

1. Legal restrictions or requirements that impact the Team?

RECOVERY PHASE MEF ISSUES

Pre-Event Phase	Response Phase	**Recovery Phase**	Reconstitution Phase
Team Issues	Team Issues	Team Issues	Team Issues
MEF Issues	MEF Issues	**MEF Issues**	MEF Issues

FUNCTIONAL AREA ISSUES

COMMAND AND CONTROL. ***HAVE YOU CONSIDERED:***

1. How the event might change the Command and Control environment?

2. Standard communications capability to provide incident command and control?

3. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation to MEFs?

4. Procedures to receive, analyze, and authorize recovery actions in a timely manner?

5. Methods to concurrently manage both the organization and recovery?

6. Procedures to inform members of the organization, supported and supporting organizations, customers, and stakeholders of the status of recovery operations?

7. Mechanisms to forecast the completion of recovery operations in order to more quickly transition to full operations

8. The aspects, sequencing and timing to recover various operations?

OPERATIONS. ***HAVE YOU CONSIDERED:***

1. How the event might change the Operations environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of operations capabilities on MEFs?

3. The criteria to determine whether to recover or replace the MEF and the procedures to report this information to the CM Team?

4. The prioritization of recovery of MEF capabilities?

5. Providing the Recovery Team with primary and alternate contact information for the following?

    - Key people for each MEF

- Supporting contractors
- Contingency support providers
- Suppliers
- Facility managers/owners

6. The priority of effort to maintain MEFs within operations?

7. The aspects, sequencing and timing to recover all operations?

HUMAN RESOURCES AND PUBLIC RELATIONS. ***HAVE YOU CONSIDERED:***

1. How the event might change the Human Resources and Public Relations environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of HR support to MEFs?

3. The requirements and processes necessary to recover the Human Resource support of the MEF?

4. Requirements for cleared personnel necessary to recover MEFs, including alternates as appropriate?

5. Procedures to coordinate movement and action with first responders, law enforcement, and Recovery Teams?

6. Updating all members, business partners and the public as to the status of the recovery effort?

7. The priority of effort to maintain MEFs within Human Resources and Public Relations?

8. Access to the necessary points of contact to support or recover MEFs?

9. The aspects, sequencing and timing to recover Human Resources and Public Relations?

SECURITY. ***HAVE YOU CONSIDERED:***

1. How the event might change the Security environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of security support to MEFs?

3. Procedures to interact with local/state/federal security/authorities in support of recovery effort?

4. The security properties of each MEF as well as any security requirements particular to support MEF recovery? Issues may include the following:

   - Security clearances for internal and external staff (contractors, suppliers, visitors VIPs, federal, state and local officials),
   - Secure access,
   - Secure communication of classified material,
   - Handling procedures for classified material,
   - Ensure that plans and commitments are in place to provide for security during evacuation of personnel and classified material and documents.

5. Procedures to assess and implement changes in security requirements caused by the event?

6. Procedures to ensure that all replacement equipment, software, and services have proper security certifications, capabilities and authorizations prior to use?

7. Identity control for all recovery team personnel, to include access badging or use of identity vests, etc.?

8. The priority of effort to maintain MEFs within Security?

9. The aspects, sequencing and timing to recover Security?

COMMUNICATIONS. ***HAVE YOU CONSIDERED:***

1. How the event might change the Communications environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of communication support to MEFs?

3. The communication characteristics of each MEF as well as any communication requirements particular to support MEF recovery?

4. The priority of effort to maintain MEFs within Communications?

5. Security of classified communications material, assets, etc.?

6. The communications resources and assets necessary to support restoration of the MEF?

7. The aspects, sequencing and timing to recover Communications?

FACILITIES. ***HAVE YOU CONSIDERED:***

1. How the event might change the Facilities environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of facility support to MEFs?

3. The aspects, sequencing and timing to recover Facilities?

4. Criteria and procedures to determine and report any requirement to activate or relocate an alternate site?

5. Criteria and procedures to determine and report whether recovery or reconstitution is possible at the primary site?

6. The priority of effort to maintain MEFs within Facilities?

7. Primary and alternate personnel, skill sets, and organizational requirements to operate the primary or alternate facility 24x7 as required to recover MEFs?

8. Temporary facility requirements to support events of scale in terms of food, shelter, office, construction space, water, sanitation, sewage, etc.?

9. Providing the Recovery Team with maps, plans, blue prints, drawings, diagrams, software media, etc.?

10. The identification of and restricted access to buildings and areas damaged or contaminated by the event?

UTILITIES. ***HAVE YOU CONSIDERED:***

1. How the event might change the Utilities environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of utilities support to MEFs?

3. The technical specifications of the utilities capabilities that support the MEFs, and the processes necessary for their recovery?

4. Coordinating critical utility requirements with local utility providers?

5. Alternate utility providers and sources that may support MEF recovery?

6. Coordinating utility restoration with utility providers?

7. Recovery Team access to utility systems, installation drawings, and manuals that display critical features such as the following?

    - Valves,
    - Controls/control panels,
    - Contacts,
    - Circuit breakers,
    - Cutoffs and bypasses etc.
    - Communications equipment,
    - Security devices,
    - HVAC,
    - Fire warning, fire suppression, and
    - IT/IS resources such as Computing and Networking H/W and S/W, peripherals, and support ser vices.

8. External utility expertise capable of supporting MEF utilities recovery?

9. Mobile utility sources to support recovery operations, e.g., fuel, power, decontamination, water, etc.?

10. Short-term HAZMAT collection and storage sites for solid and liquid HAZMAT pending post-event long-term disposition?

11. The priority of effort to maintain MEFs within Utilities?

12. The aspects, sequencing and timing to recover Utilities?

OPERATIONAL EQUIPMENT. ***HAVE YOU CONSIDERED:***

1. How the event might change the Operational Equipment environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation

of operational equipment support to MEFs?

3. The technical specifications and requirements for the operational equipment supporting MEFs, and the process to recover the equipment's capability?

4. Alternate sources of equipment with external contractors and suppliers to include name, address, telephone, website, and e-mail?

5. Procedures and restrictions for obtaining short-term replacement equipment (rental or lease)?

6. MOUs as required with other locales to provide short-duration replacement/augmentation equipment to support each MEF?

7. Equipment recovery criteria and processes?

8. The priority of effort to maintain MEFs within Operational Equipment?

9. The aspects, sequencing and timing to recover Operational Equipment?

TRANSPORTATION. ***HAVE YOU CONSIDERED:***

1. How the event might change the Transportation environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of transportation support to MEFs?

3. MEF-related transportation requirements and the processes to recover the transportation capability, to include the following?

    - Transportation alternatives,
    - Transport to and from event,
    - Transportation to and from alternate site,
    - External transportation requirements to fill internal shortfalls,
    - Security of transportation assets,
    - Transportation of classified documents, equipment, etc.,
    - Funding and sourcing replacement transportation equipment,
    - Spare Part replenishment,
    - Tools.

4. The priority of effort to maintain MEFs within Transportation?

5. The capabilities of in-house transportation providers and external local, state, and federal transportation agencies?

6. Routes and traffic control measures to deconflict the needs of internal and external Response and Recovery teams? In particular, have you considered coordinating the movement of the following?

    - Response and Recovery Teams,
    - Contractor vehicles and equipment operating in support of MEF recovery,
    - Security personnel,
    - Classified documents and equipment,
    - Evacuation of base and/or local population.

7. Using any internal rolling stock and emergency vehicles to support the Recovery Phase?

8. The criteria and processes to recover transportation capabilities?

9. Requirements and procedures to augment or recover equipment, services, routes and local Department of Transportation authority to move?

10. The aspects, sequencing and timing to recover Transportation?

SUPPORT SERVICES. ***HAVE YOU CONSIDERED:***

1. How the event might change the Support Services environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of support services to MEFs?

3. The processes to recover the support services that support MEFs?

4. Contact lists of external and internal service providers (and alternates) to include name, telephone, address, and e-mail address, in support of the recovery process? Refer to Human Resources – Consequence Management, Table III-2 for applicable contact data.

5. Multiple sources for internal and external services necessary to support MEFs?

6. Security requirements for the services that support MEFs, to include the following?

    - Physical security requirements,

- Requirements for guards and couriers,
- Secure access requirements and procedures,
- Secure communication and handling procedures for classified material,
- Plans and commitments to provide for security during the evacuation of personnel, classified material, and documents.

7. Multi-source contract vehicles in support of equipment, supplies and services necessary to sustain MEFs?

8. The contracting authority (with alternate) able to meet service contract requirements in support of recovery effort?

9. Identifying the procedures to recover support services?

10. The priority of effort to maintain MEFs within Support Services?

11. The aspects, sequencing and timing to recover Support Services?

IT/IS. ***HAVE YOU CONSIDERED:***

1. How the event might change the IT/IS environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of IT/IS support to MEFs?

3. The IT/IS requirements necessary to recover the MEFs, as well as the processes to recover the IT/IS capability?

4. Access to a copy of current IT/IS equipment inventory, use, and assignment for reference in developing equipment requirements for recovery of IT/IS functions?

5. A list of all IT sources and suppliers that support the MEF, to include name, address, website, e-mail, telephone, part/model numbers, etc.?

6. The IT environment's physical and cyber security and for security of classified material and equipment supporting the MEF such as the following?

    - Facility access,
    - Facility intrusion/detection,
    - IT/IS equipment hardware and peripherals,

- Operating System (OS) software,
- Application software,
- Data access,
- IT intrusion:
  - IT intrusion/detection,
- Unauthorized software access attempts,
- Data theft,
- Data destruction.
- Encryption devices,
- Vital records, data backup and recovery system (mirror, tape, etc.) to ensure MEF viability.

7. Provisions to identify and backup vital records, data, and systems (mirror, tape, etc.) to recover MEF?

8. The Recovery Team IT/IS equipment requirements to include the following?

- Design/development tools as required to include laptop/workstations,
- Equipment inventory (other than IT/IS equipment and communication, (separate list)), required by the Recovery Team to repair, recover or relocate the IT/IS capability that supports the MEF,
- Plans and drawings.

9. Establishing IT/IS requirements for the following?

- Access to Data Center,
- Requirements for alternate site (Hot, Warm, or Cold Site.)
- Characteristics of data moved to the alternate site, including timelines to upload and staff,
- Hardware and peripherals,
- OS software,
- Application software,
- Vital records and data backup including frequency,
- Maintenance,
- Power source,
- HVAC,
- Connectivity source,
- Alternatives and backups for all of the above.

10. The recall of essential IT/IS Personnel?

11. MEF IT/IS security requirements, to include the following?

    - Security clearances for internal and external personnel (contractors, suppliers, visitors, VIPs, federal, state and local officials),
    - Secure access,
    - Secure communication and handling of classified material,
    - Plans and commitments are in place to provide for security during evacuation of personnel and classified material and documents.

12. The IT/IS resources and assets necessary to support the restoration of the MEF?

13. Criteria and processes to recover IT/IS services?

14. The priority of effort to maintain MEFs within IT/IS?

15. The aspects, sequencing and timing to recover IT/IS?

FISCAL, CONTRACTING AND PURCHASING. ***HAVE YOU CONSIDERED:***

1. How the event might change the Fiscal, Contracting and Purchasing environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of Fiscal, Contracting, and Purchasing support to MEFs?

3. Multi-source contract vehicles in support of equipment, supplies and services necessary to sustain MEFs?

4. A contracting authority (with alternate) able to meet service contract requirements in support of recovery effort?

5. Procedures to estimate and budget the funding requirements required to staff, train, and equip the Response Team in support of the MEF?

6. Procedures to provide fiscal support and accounting for the actions required in the recovery effort?

7. Criteria and processes to recover or replace Environmental, Health and Safety services?

8. The priority of effort to maintain MEFs within Fiscal, Contracting and Purchasing?

9. The aspects, sequencing and timing to recover Fiscal, Contracting and Purchasing?

10. Budget and funding requirements to staff, train and equip the Recovery team?

11. Procedures to obtain sufficient funds to support response operations?

12. Regulations and procedures to capture costs of response operations?

ENVIRONMENTAL, HEALTH AND SAFETY. ***HAVE YOU CONSIDERED:***

1. How the event might change the Environmental, Health and Safety environment?

2. Procedures to update, validate, and report the Response Team's initial assessment of the impact of loss or degradation of Environmental, Health and Safety support to MEFs?

3. The recall of Environmental, Health and Safety service providers?

4. The characteristics of Environmental, Health and Safety service requirements necessary to recover MEFs, as well as the process to recover their capabilities?

5. All equipment, communications, facility, transportation, detection devices, kits for HAZMAT agents, protective equipment, and decontamination material required to support and recover the MEF?

6. Multiple internal and external sources for Environmental, Health and Safety services that support MEFs?

7. Prioritizing Environmental, Health and Safety support to recover MEFs?

8. Listing external and internal Environmental, Health and Safety service providers, including alternates, to support MEF recovery, including names, telephone, address, and e-mail?

9. Multi-source contract vehicles in support of Environmental, Health and Safety equipment, supplies and services necessary to recover MEFs?

10. A primary and alternate contracting authority to meet Environmental, Health and Safety services contract requirements in support of recovery effort?

11. Criteria and processes to recover or replace Environmental, Health and Safety services?

12. The priority of effort to maintain MEFs within Environmental, Health and Safety?

13. The aspects, sequencing and timing to recover Environmental, Health and Safety?

FIRST RESPONDER. ***HAVE YOU CONSIDERED:***

1. How the event might change the First Responder environment?

2. Liaison to ensure unimpeded support of First Responders during the Recovery phase?

3. A full accounting of organization and First Responder property prior to the departure of First Responders?

LEGAL. ***HAVE YOU CONSIDERED:***

1. How the event might change the Legal environment?

2. Procedures for the legal staff, internal or external, to have access to key records and files needed to continue or resume ongoing efforts?

3. External legal assistance in the event the workload overcomes the primary staff?

4. Legal assistance to the other functional areas that might anticipate legal issues? To include:

    - Operations
    - Command and Control
    - Human Resources and Public Relations
    - Environmental Health and Safety
    - Fiscal, Contracts and Purchasing

5. The priority of effort to maintain MEFs within the Legal functional area?

RECONSTITUTION PHASE

The purpose of the Reconstitution Phase is to provide structure and purpose to senior leadership in planning for replacement of MEFs lost as a result of either natural or man-made disasters. In laying the groundwork for possible reconstitution, CM planners support the decision process several levels up. The Reconstitution Phase addresses the following key questions:

- **Do we rebuild the MEF as it existed before the disaster, or**
- **Do we leverage emerging technology through the Research and Development process to improve performance, enhance security and remedy additional threats or hazards?**

RECONSTITUTION PHASE TEAM ISSUES

PRE-EVENT PHASE	RESPONSE PHASE	RECOVERY PHASE	**RECONSTITUTION PHASE**
TEAM ISSUES	TEAM ISSUES	TEAM ISSUES	**TEAM ISSUES**
MEF ISSUES	MEF ISSUES	MEF ISSUES	MEF ISSUES

The Reconstitution Team should develop the Reconstitution Plan. The level of detail and operational requirement documents necessary to provide leadership with the ability to commence MEF reconstitution is a function of the complexity of the organization, the strategic environment, and technology in general. The Reconstitution Team must remain flexible and constantly incorporate the latest state of the art enhancements for physical, cyber, and technical features that improve MEF performance, security and survivability. The Reconstitution Team has no particular Functional Area issues to consider, since they perform their tasks in a normal day to day environment.

RECONSTITUTION PHASE MEF ISSUES

PRE-EVENT PHASE	RESPONSE PHASE	RECOVERY PHASE	**RECONSTITUTION PHASE**
TEAM ISSUES	TEAM ISSUES	TEAM ISSUES	TEAM ISSUES
MEF ISSUES	MEF ISSUES	MEF ISSUES	**MEF ISSUES**

FUNCTIONAL AREA ISSUES

COMMAND AND CONTROL. ***HAVE YOU CONSIDERED:***

1. Emerging Command and Control procedures, technology, or systems that may better allow you to retain the initiative for both the event and organizational operations?

2. Changes in the Defense environment that impact locations, procedures, and external dependencies.

3. How reconstitution supports strategic plans?

4. Approval of the reconstitution plan by senior leadership?

OPERATIONS. Given the future-based focus of MEF reconstitution and the pace of technological innovation, the Reconstitution Phase may remain somewhat vague and focus more on conceptual requirements rather than existing specific requirements. ***BUT HAVE YOU CONSIDERED:***

1. A thorough analysis based on current and emerging trends in the following areas?
    - Research and Development focus,
    - Engineering and Quality standards, and
    - Emerging Performance Specifications.
2. Documenting and benchmarking current operations against known DOD, DON, and industry best practices?
3. Briefing the Reconstitution phase to applicable Research and Development people, and functional area managers?
4. How reconstitution of operations supports the strategic goals two levels up.

FIRST RESPONDERS. ***HAVE YOU CONSIDERED:***

1. Including a First Responder review of the Reconstitution effort?
2. The availability and performance record of local First Responders in the reconstitution process?

FOR EACH OF THE REMAINING FUNCTIONAL AREAS, HAVE YOU CONSIDERED:

1. Documenting and benchmarking current Human Resource processes against DOD and industry best practices?
2. How reconstitution of Human Resources and Public Relations support strategic requirements?

APPENDIX E: CONSEQUENCE MANAGEMENT PLAN FORMAT

Appendix E: Consequence Management Plan Format

Classification/For Official Use Only
Office Code
Date
Consequence Management Plan for [Installation Name]

Ref: (a) List any pertinent references to this plan

1. **SITUATION**

a. General. Provide a short summary of the organization, it's mission and vision, and how this plan supports that mission.

b. Threats and Vulnerabilities. Provide a short but complete summary of the known physical and cyber threats and vulnerabilities facing the organization.

c. Support. Provide a short summary of the internal and external support available to the organization, to include other First Responders, critical vendors, etc, as well as supported and supporting DoD organizations.

d. Participants in the Plan. This paragraph provides a short summary of who within the organization participates in this particular plan. It will highlight any part of the organization that does not participate due to physical location, etc., as well as those internal and external organizations that are included, such as any support contractor personnel co-located with the organization, etc.

e. Assumptions. Provide a short summary of the assumptions that frame the organization's planning perspective (e.g.: notice or no-notice activation, duration of the plan, use of alternate locations, reliance upon external supporters, etc.)

2. **MISSION**. Clear, concise one-paragraph statement of tasks; what is to be accomplished by the organization as a whole; who, where, when, and so much of the why as necessary for intelligent coordination and cooperation.

3. EXECUTION

a. Intent. This paragraph states the over-arching intent during execution of the plan and gives provides personnel a goal to focus upon if precise guidance is unavailable once an event occurs that triggers the plan.

b. Concept of Operations. Provide a summary statement of how the plan will be conducted to accomplish the goal. It includes a discussion on the four phases of the Plan (Pre-event, Response, Recovery, and Reconstitution), to include:

(1) Pre-event Phase. The Pre-event phase is the normal phase for day to day operations. It includes periodic training and exercises, continual evaluation and improvement of processes, updates to information, and outfitting key individuals with proper equipment. Additionally, it involves discussions between the staff and First Responders, supporting organizations, etc, to increase overall awareness and decrease confusion and friction during execution. The Pre-event phase ends when an event triggers execution of the plan. When the event has concluded, the organization returns to the Pre-event phase, assesses any lessons learned, and prepares for another event.

(2) Response Phase. The Response Phase starts with an initiating event; the organization may or may not have forewarning of this event. A call for Emergency Responders may typically initiate this phase. The focus of main effort during this phase is preserving life and limb, personnel accountability, and limiting damage to infrastructure. This phase may take place concurrent with the Recovery Phase. First Responders will normally assume command of the incident during this phase and will designate an "Incident Commander"; the (designated person) is the DON representative who will coordinate actions during this phase in support of First Responders. The Response Phase is complete when the following conditions are met:

(a) First Responders complete their on-scene actions and return control of the infrastructure to responsible officers; and

(b) All personnel are accounted for, to include notification of family members and next of kin.

(c) Mission Essential Functions are stabilized; and

(d) Contact with key organizations and individuals is confirmed or reestablished.

(3) Recovery Phase. The Recovery Phase starts when existing or developing conditions indicate that the organization is able to begin restoring functionality of the physical and cyber infrastructure necessary to sustain normal operations. The focus of main effort during this phase is restoring Mission Essential Functions. The (designated person) is in charge during this phase and coordinates action with the staff responsible for ongoing operations. The Recovery Phase is complete when the following conditions are met:

(a) Mission Essential Functions are restored; and

(b) The organization resumes normal operations; and

(c) Reconstitution requirements are identified and incorporated with the Reconstitution Plan.

(4) Reconstitution Phase. The Reconstitution Phase may start as soon as it is possible to develop detailed damage or loss reports indicating the extent of damage done to the organization and need not wait until normal operations have resumed. The focus of main effort during this phase is gaining and maintaining momentum to either reconstitute damaged or lost infrastructure in an "as was" state or in a "to be" state, dependent on damage or loss assessments, strategic goals, and emerging applicable technology.
The Reconstitution Phase may take months or years to complete and may require significant investment of resources after approval at the appropriate level. The (designated position) is in charge of this phase, and will coordinate within the chain of command and with supported and supporting organizations.
Reconstitution is complete when the following conditions are met:

(a) Damaged or lost infrastructure is replaced; and

(b) Policies and procedures are modified to reflect the new infrastructure requirements; and

(c) Operational stability is regained.

c. Plan Execution Triggers. This paragraph sets forth the events that trigger executing the plan. It includes triggers for notice and no-notice execution, decision points used to determine whether to execute the plan, and coordination with supported, supporting, higher, lower and adjacent organizations, as well as Federal, State, or local entities.

d. Mission Essential Functions. This paragraph contains a short concise listing of each of the functions that are critical to mission assurance.

e. Vital Records and Databases. The protection and ready availability of electronic and hardcopy documents, references, records, and information systems needed to support mission essential functions under the full spectrum of emergencies is another critical element of the CM plan. Personnel must have access to and be able to use these records and systems in conducting their mission essential functions. Categories of these types of records may include:

(1) Emergency Operating Records. Vital records, regardless of media, essential to the continued functioning or reconstitution of the organization during and after an emergency. Included are emergency plans and directives; orders of succession; delegations of authority; staffing assignments; and related records of

a policy or procedural nature that provide the staff with guidance and information resources necessary for conducting operations during an emergency, and for resuming normal operations at its conclusion. The organization's Personnel Roster, Location Diagrams, and Building Diagrams are examples of Emergency Operating Records.

(2) Legal and Financial Records. Vital records, regardless of media, that are critical to the essential legal and financial functions and activities, and protecting the legal and financial rights of individuals directly affected by unit activities. Included are records having such value that their loss would significantly impair the conduct of essential functions, to the detriment of the legal or financial rights or entitlements of the organization or of the affected individual. Examples of this category of vital records are accounts receivable; contracting and acquisition files; official personnel files; payroll, retirement, and insurance records; and property management and inventory records.

f. Tasks. Each subordinate office, section, or unit within the organization, along with any external plan participant, is assigned a separate numbered paragraph containing tasks to be carried out during each phase of the plan (Pre-Event, Response, Recovery, and Reconstitution).

g. Coordinating Instructions. Contains instructions common to two or more activities, offices, or sections, coordinating details and control measures applicable to the organization as a whole, and time and conditions when the plan is to be implemented. Essential elements of information may be listed for emphasis.

4. ADMINISTRATION AND LOGISTICS

This paragraph contains logistics, human resources, and administrative policies and instructions for implementing the plan. It refers the reader to Annex E for further details.

5. COMMAND AND SIGNAL

a. Command. This paragraph summarizes the succession of leadership within the organization. Copies of the Succession Letters are contained in Annex E, Administration and Logistics.

b. Implementation Procedures. This paragraph summarizes the implementation procedures for an announced and unannounced implementation of the plan. Additionally, provides pre-determined conditions that signal moving from one phase of the plan to another (e.g.: Pre-Event to Response, or from Response to Recovery, etc.)

c. Locations of Key Personnel. This paragraph summarizes the locations of key people during the various phases of the plan.

//signed//

Commander

Annexes:

A – Pre-Event Plan

B - Response Plan

C – Recovery Plan

D – Reconstitution Plan

E – Administration and Logistics

Distribution:

ANNEX A

PRE-EVENT PLAN

1. **MISSION.** Clear, concise one-paragraph statement of tasks during the Pre-event Phase; what to be accomplished by the organization as a whole; who, where, when, and so much of the why as necessary for intelligent coordination and cooperation.

2. **CONCEPT OF PRE-EVENT ACTIONS.** The Pre-event Phase starts upon signature of the CM Plan. The focus of main effort during the Pre-event Phase is training and exercises to build awareness of the Plan, and establishing CM as an integral part of conducting normal operations.

3. **ACTION**

   a. **Tasks**

      (1) Leadership

      List tasks assigned to designated commanders/leaders during the Pre-event phase

      (2) Consequence Management Lead

      List tasks assigned to the CM Team leader during the Pre-Event phase

      (3) Key Operational Positions

      List tasks of key individuals during the Pre-event phase

      (4) Emergency Operations Team

      List tasks assigned to the team comprising the Emergency Operations Center during the Pre-event phase

      (5) Other Personnel

      Lists tasks assigned to others within the organization during the Pre-Event phase

b. <u>Coordination</u>. Contains detailed instructions for coordinating actions, to include:

(1) First Responders

(2) Rescue Teams

(3) Family Members

(4) Higher, lower, adjacent

(5) Media

(6) External Support

(7) Key Personnel

(a) Response Lead

(b) Pre-Event

(c) Recovery Lead

(d) Command

(c) Key Operational Positions

(d) Emergency Operations Team

(8) Other Members of the Organization

5. <u>LOCATION OF KEY PERSONNEL</u>. Contains preplanned and rehearsed locations for Key Personnel during the Pre-Event Phase.

a. Organizational Leadership

b. Response Lead

c. Recovery Lead

d. Key Operational Positions

e. Emergency Operations Team

ANNEX B

RESPONSE PLAN

1. **MISSION.** Clear, concise one-paragraph statement of tasks during the Response Phase; what to be accomplished by the organization as a whole; who, where, when, and so much of the why as necessary for intelligent coordination and cooperation.

2. **CONCEPT OF RESPONSE OPERATIONS.** The Response Phase starts with an initiating event; the organization may or may not have forewarning of this event. A call for Emergency Responders may typically initiate this phase. The focus of main effort during this phase is preserving life and limb, accounting for people, and limiting damage to infrastructure. First Responders (internal or external) will assume command of the incident during this phase and will designate an "Incident Commander"; the organizational representative (designated person) will coordinate actions during this phase in support of First Responders.

3. **RESPONSE PLAN IMPLEMENTATION TRIGGERS.** This paragraph sets forth the events that trigger implementing the Response Plan, including triggers for notice and no-notice execution. It details any decision processes used to determine whether to implement the plan, and coordination with higher, lower and adjacent organizations, and Federal, State, or local entities.

4. **ACTION**

   a. **Response Lead.** (Designated person; alternate(s))

   b. **Tasks**

      (1) Evacuation procedures

      (2) Muster location, procedures, and reporting

      (3) Activation of Emergency Operations Center and the Emergency Operations Team

      (4) Key Personnel

         (a) Leadership

         (b) Response Lead

         (c) Key Operational Positions

         (d) Emergency Operations Team

(5) Other Members of the organization

c. <u>Coordination</u>. Contains detailed instructions for coordinating actions in support of the Response Plan, to include:

(1) First Responders

(2) Rescue Teams

(3) Family Members

(4) Higher, lower, adjacent

(5) Media

(6) External Support

(7) Key Personnel

(a) Pre-Event Lead

(b) Response Lead

(c) Recovery Lead

(d) Leadership

(c) Key Operational Positions

(d) Emergency Operations Team

(8) Other Members of the organization

5. <u>CRITERIA FOR TERMINATING THE RESPONSE PHASE</u>. The Response Phase is complete when the following conditions are met:

a. First Responders complete their on-scene actions and return the infrastructure to organizational control; and

b. All personnel are accounted for, to include notification of family members and next of kin; and

c. The immediate crisis situation has been stabilized, with initial plans for Recovery complete or underway.

6. **LOCATION OF KEY PERSONNEL.** Contains preplanned and rehearsed locations for Key Personnel during the Response Phase.

   a. **Leadership**

   b. **Response Lead**

   c. **Recovery Lead**

   d. **Key Operational Positions**

   e. **Emergency Operations Team**

ANNEX C

RECOVERY PLAN

1. **MISSION.** Clear, concise one-paragraph statement of tasks during the Recovery Phase; what to be accomplished by the organization as a whole; who, where, when, and so much of the why as necessary for intelligent coordination and cooperation.

2. **CONCEPT OF RECOVERY.** The Recovery Phase starts when the Emergency Response Team determines that existing or developing conditions indicate that the organization is able to start restoring functionality of the physical and cyber infrastructure necessary to sustain normal operations. The focus of main effort during this phase is restoring Mission Essential Functions. The (designated person) is in charge during this phase and coordinates action with the Response and Pre-Event Leads.

3. **RECOVERY PLAN IMPLEMENTATION TRIGGERS.** This paragraph sets forth the events that trigger implementing the Recovery Plan. It includes instructions for any decision points used to determine whether to implement the Recovery Plan, and includes coordination with higher, lower and adjacent organizations, or Federal, State, or local entities.

4. **PRIORITY OF EFFORT.** This paragraph establishes pre-planned priorities for recovering cyber and physical systems. It is used by the Recovery Team to focus their efforts in order to recover the most important systems before less important systems.

5. **ACTION**

    a. Recovery Lead. (Designated person; alternate(s))

    b. Tasks

        (1) Leadership

        (2) Recovery Lead

            (a) Activate Recovery Team

            (b) Restore systems and processes

        (3) Key Operational Positions

            (a) Muster location, procedures, and reporting

            (b) Prepare backup documents

(4) Emergency Operations Team

(a) Assess operational condition of the organization

(b) Recommendation for use of alternate site

(5) Other Members of the Organization

c. Coordination. Contains detailed instructions for coordinating actions, to include:

(1) First Responders

(2) Rescue Teams

(3) Family Members

(4) Higher, lower, adjacent

(5) Media

(6) External Support

(7) Key Personnel

(a) Response Lead

(b) Pre-Event Lead

(c) Recovery Lead

(d) Leadership

(c) Key Operational Positions

(d) Emergency Operations Team

(8) Other Members of the Organization

6. CRITERIA FOR TERMINATING THE RECOVERY PHASE. The Recovery Phase is complete when the following conditions are met:

a. Mission Essential Functions are operational; and

b. The organization resumes normal operations; and

c. Reconstitution requirements are identified and incorporated with the Reconstitution Plan.

7. **LOCATION OF KEY PERSONNEL.** Contains preplanned and rehearsed locations for Key Personnel during the Recovery Phase.

   a. **Leadership**

   b. **Response Lead**

   c. **Pre-Event Lead**

   d. **Recovery Lead**

   e. **Key Operational Positions**

   f. **Emergency Operations Team**

ANNEX D

RECONSTITUTION PLAN

1. **MISSION.** Clear, concise one-paragraph statement of tasks during the Reconstitution Phase; what to be accomplished by the organization as a whole; who, where, when, and so much of the why as necessary for intelligent coordination and cooperation.

2. **CONCEPT OF RECONSTITUTION.** The Reconstitution Phase may start as soon as it is possible to develop detailed damage or loss reports indicating the extent of damage to the organization and need not wait until normal operations have resumed. The focus of main effort during this phase is gaining and maintaining momentum to either reconstitute damaged or lost infrastructure in an "as was" state or in an "to be" state, depending on damage or loss assessments, strategic goals, and emerging applicable technology. The Reconstitution Phase may take months or years to complete and may require significant investment of resources following approval at the appropriate level. A senior member of the staff is normally in charge of this phase, and will coordinate this phase within the chain of command and in coordination with supported/supporting organizations.

3. **RECONSTITUTION PLAN IMPLEMENTATION TRIGGERS.** This paragraph sets forth the conditions necessary to implement the Reconstitution Plan, including instructions for any decision points used to determine whether to implement Reconstitution, and coordination with higher, lower, adjacent, or Federal, State, or local entities.

4. **ACTION**

a. **Reconstitution Lead.** (Designated person; alternate(s))

b. **Tasks**

(1) Leadership

(2) Reconstitution Lead

(3) Key Operational Positions

(4) Other Members of the Organization

c. **Coordination.** Contains detailed instructions for coordinating actions, to include:

(1) Key Personnel

(a) Leadership

(b) Key Positions

(c) Other Members of the Organization

5. CRITERIA FOR TERMINATING THE RECONSTITUTION PHASE.

The Reconstitution Phase is complete when the following conditions are met:

a. Damaged or lost infrastructure is replaced; and

b. Policies and procedures are modified to reflect the new infrastructure requirements; and

c. Operational stability is regained.

ANNEX E

ADMINISTRATION AND LOGISTICS

Notional Timeline for Events

Evacuation Plan and Procedures

Succession Letters

Recall Rosters and Procedures

Consequence Management Team Assignments

Locations of alternate facilities

Reports in support of the Plan

Prioritized List of Critical Cyber and Physical Infrastructures

List of Contractors and Service Agents in Support of Critical Infrastructures

Map of Company Area(s)

Building Plans of Critical Infrastructures

List of Critical Records and Documents

List of Critical Information Systems

APPENDIX F: EXERCISES

APPENDIX F: EXERCISES

1. **PURPOSE:** This Appendix provides guidance on how to organize and plan to conduct an exercise to test the adequacy of CM Plans, and evaluate the organization's ability to execute the Plan.

2. **TYPES OF EXERCISES:**

   - **Notice:** In this exercise all participants are made aware of the exercise dates/times, the objectives, general areas to be exercised and evaluated, and a general sequence of events.

   - **No-Notice:** In a no-notice exercise all, or a portion of, the organization is not made aware of the date or time of the exercise. The focus is evaluating and training the organization in executing the CM Plan, with emphasis on Response.

   - **Table-Top:** involves a limited number of people, usually focused on leaders, decision makers, and other key personnel, and focuses on exercising management control. Table-Top exercises are cost-effective and often employ simulation and 'war-gaming' to facilitate 'real-time' decision analysis.

   - **Communications:** Tests primary and back-up communications plans, and the organizations' ability to maintain communications through disruptive events or conditions.

3. **REQUIREMENTS**:

   a. People. The following temporary organization is recommended to plan and conduct the exercise, regardless of exercise scope or duration:

Exercise Control Cell. Plans, implements, and evaluates the exercise. The Control Cell:

- develops exercise objectives,
- identifies the specific elements of the CM Plan to be evaluated.
- writes the exercise plan

- conducts and monitors the exercise,
- evaluates performance and captures lessons learned, and
- prepares an after-action report with recommended corrective actions.

The Control Cell will normally consist of a Senior Exercise Controller and any number of controller assistants as necessary to observe each participating group/activity in the exercise. Assistant Controllers should have appropriate subject matter expertise to evaluate the various functional areas to be exercises/tested.

External Element. These Control Cell members represent external agencies/conditions that exert an influence on the organization (First Responders, adjacent, higher and subordinate organizations, supported and supporting units, Suppliers, environmental conditions, other factors). The External Element operates independent of, but reports to, the Senior Controller. In less demanding exercises, the Control Cell may perform these functions.

b. Plans. The following products are recommended to support the exercise:

Scenarios:

A scenario sets the conditions under which exercise events take place and provides a basis for future exercises. A scenario template is at Tab A, and a Sample scenario is at Tab B.

Exercise Plan: The Exercise Plan can follow any format, although the format contained in Appendix F is well suited, and is recommended. At a minimum the exercise plan should:

- establish the authority for the exercise, and who will be in charge of conducting it
- establish the date and times (Notice), and purpose of the exercise
- identify exercise participants and their roles
- list each exercise objective
- identify support requirements and who will fulfill them
- describe the exercise scenario and general flow of events
- provide guidance for capturing and reporting after action items

Master Scenario Events List (MSEL): The MSEL identifies each pre-planned event scheduled to take place and the exact time it will occur. The MSEL is developed based on exercise/MEF evaluation objectives, and describes the nature of the event in sufficient detail to allow exercise participants to respond. The MSEL is kept close-hold in both Notice and No-Notice exercises. In larger organizations, or when employing a more complex exercise, a separate MSEL may be used for the Exercise Control Cell and the External Element. MSELs can be designed to test a process (sequencing, supportability, effectiveness, etc), the participant's ability and readiness to perform that process, and to require a decision or series of decisions.

Only designated participants are made aware of the contents of the MSEL lists (honest brokers) in order to maintain the integrity of the exercise. A sample MSEL list is at Tab C.

3. **DEVELOPING THE EXERCISE.** The CM team provides an excellent planning forum for CM exercise development. Some considerations in CM exercise development include:

a. The exercise purpose should be stated to identify the goals to be achieved, and their priority. Exercises are useful in evaluating the CM Plan, evaluating people's ability to carry out elements of those plans, and to train and educate people about the Plan and their role in its execution.

b. Specific exercise objectives should be identified within functional areas and/or phases in as much detail as possible.

c. Metrics for performance measurement and establishing a basis for after-action reporting and follow-up requirements.

d. External participation requirements/desires. CM Plans will not be executed in a vacuum, and exercises should strive to reflect realistic participation of outside agencies.

e. Consider personnel and support requirements early. Exercises require significant lead time to ensure all the required elements are in place without undo interference with business operations. Include people, logistics, communications, and external requirements in the exercise timeline.

f. Consider the timing and tempo of the exercise in the context of the objectives. MSEL events should reflect realistic conditions, and allow for sufficient time for participants to meet the training objectives.

TAB A: SCENARIO TEMPLATE

This Tab provides a template to develop an exercise scenario. When completed it provides a basis for developing detailed exercise plans and supporting analysis.

Scenario # _____

Background: Determine the conditions that will best support exercise objectives.

Environmental Conditions:

Time of Year: _____

Time of Day: _____

Day of Week: _____

Weather Conditions: _____

Temp: _____

Precip: _____

Winds: _____

Travel Conditions:

Road: _____

Rail: _____

Mass Transit: _____

Air: _____

Traffic Conditions: _____

Local activities underway: _____

Operating Conditions:

Operational Tempo:(normal/above/below) _____

During/After Working Hours: _____

Weekday/Weekend/Holiday: _____

Number of personnel (military/civilian):

On travel: _____

Sick: _____

On Leave: _____

Key Personnel Status: _____

Situation: Establish the conditions under which the organization is operating at the time the exercise commences, e.g.: normal flight operations with utilities and support services operating normally. Consider scenario factors that will affect exercise objectives, such as status of contracted support, threat conditions, and missions currently planned or underway.

TAB B:SAMPLE SCENARIO – NAS SOUTHSIDE

Scenario # 1-ND-03

Background:

Environmental Conditions:

Time of Year: Fall/Winter

Time of Day: 0910

Day of Week: Friday

Weather Conditions: Overcast, rain predicted

Temp: 35 degrees farenheit

Precip: none

Winds: west at 3 kts

Travel Conditions:

Road: normal

Rail: normal

Mass Transit: normal

Air: minor delays

Traffic Conditions:

Off-base: pre-holiday related shopping and air travel has resulted in heavy road traffic

On-base: normal

Local activities underway: none significant

Operating Conditions:

Operating Tempo:(normal/above/below) heavy support requirements from supported deploying commands. Station activities and airfield operating at high tempo.

During/After Duty Hours: during

Weekday/Weekend/Holiday: last Friday before Christmas

Number of personnel:

On travel: 15

Sick: 4

On Leave: 8

Key Personnel Status: Ops officer SIQ

Situation, Dec 19: Above normal ops tempo for most station functions. Deployment timelines require continuous readiness of all sections, with emphasis on airfield operations and refueling. Operations officer is sick in quarters, Station CO is TAD but scheduled to arrive at the local commercial airport at 1330. At 0755 AM a light to moderate freezing rain began falling throughout the region.

TAB C: SAMPLE MASTER SCENARIO EVENTS LIST (MSEL)FOR NAS SOUTHSIDE

MSEL # 1-ND-03 Exercise Start: 0745, 19 Dec

MSEL # 1

Date/Time: Dec 19, 0755 (start + :10)

Event: Unanticipated ice storm begins, light rain freezing on contact with roads, power lines, other surfaces

MSEL intent: Cause CM planner to review CM Plan/inclement weather plan

Functional Areas Affected: All, less First Responders

MSEL # 2

Date/Time: Dec 19, 0830(start + :45)

Event: Power lines feeding Station staff offices and public works fail due to heavy ice build up, all commercially provided power lost, one emergency generator failed to start automatically, shutting down computers, lights, etc. at NAS HQ building. Airfield operations not affected.

MSEL intent: Exercise applicable provisions of CM Plan for response to power failure, data loss

Functional Areas Affected: Command & Control**,** Operations, Utilities, Support Services, IT/IS, Operational Equipment

MSEL # 3

Date/Time: Dec 19, 0920 (start + 1:35)

Event: Commercial Airport closes

MSEL intent: Prompt managers/supervisors to review near-term personnel transportation requirements/status (CO inbound)

Functional Areas Affected: HR/PR, Transportation

MSEL # 4

Date/Time: Dec 19, 0922 (start + 1:37)

Event: Station Weather Service predicts falling temperatures and continued mixed precipitation through 1800.

MSEL intent: Cause staff to review inclement weather procedures, operations requirements, personnel policies, and other station activities.

Functional Areas Affected: Command & Control, HR/PR, Operations, Security, Support Services, Environmental, Health & Safety

MSEL # 5

Date/Time: Dec 19, 0945 (start + 2:00)

Event: Regional Transit Authority announces the evening rush hour schedule will be implemented at 1300, affecting station civilian employees.

MSEL intent: Force a decision regarding early release of personnel considering operations requirements

Functional Areas Affected: Command & Control, HR/PR, Operations, Legal, Communications

MSEL # 6

Date/Time: Dec 19, 1050 (start + 3:05)

Event: All commercially sourced power lost, generators providing power for emergency functions only. No estimates from commercial power company on expected restoration times. Most internet-based data sources not available.

MSEL intent: Exercise CM Plan Response Phase procedures

Functional Areas Affected: All, less First Responders

MSEL # 7

Date/Time: Dec 19, 1052 (start + 3:07)

Event: Security manager notified by local authorities an explosion has occurred in neighboring chemical plant located 1/2 mile to the west of NAS.

MSEL intent: Exercise CM Plan Response Phase

Functional Areas Affected: Command & Control, Operations, Security, Environmental, Health & Safety

MSEL # 8

Date/Time: 19 Dec 1105 (start + 4:20)

Event: NAS notified of evacuation of areas outside the gate to the west of the station the area by first responders

MSEL intent: Exercise plans for relocating designated functions

Functional Areas Affected: All

Date/Time: 19 Dec 1159: END EXERCISE

APPENDIX G: ABBREVIATIONS & ACRONYMS

Appendix G: Abbreviations & Acronyms

CBRNE	Chemical, Biological and Radiological, Nuclear, and High Yield Explosive
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Program
CM	Consequence Management
COOP	Continuity of Operations
DOD	Department of Defense
DON	Department of the Navy
EMS	Emergency Medical Services
FSL	Federal, State & Local
GETS	Government Emergency Telecommunications System
H/W	Hardware
HAZMAT	Hazardous Materials
HVAC	Heating, ventilation, Air Conditioning
ICS	Incident Command System
I&W	Indications and Warnings
IR	Infra Red
IS	Information Systems
IT	Information Technology
LL	Land Line
MEF	Mission Essential Function
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSEL	Master Scenario Events List
N/W	Network
NBC	Nuclear, Biological or Chemical
NIMS	National Incident Management System
NMCI	Navy Marine Corps Intranet
NP V 1.0	National Plan for Information Systems Protection Version 1.0
OS	Operating System
OC	Operational Continuity
OPLAN	Operations Plan
PDA	Personal Digital Assistant
S/W	Software
TMDE	Test, Measurement and Diagnostic Equipment
TSP	Telecommunications Service Priority
UPS	Uninterruptible Power Supply
WMD	Weapons of Mass Destruction

APPENDIX H:
TERMS & DEFINITIONS

Appendix H: Terms & Definitions

The following terms and definitions are as defined in SECNAV INST 3501.1 of 16 June 2002 except for those noted with an asterisk (*). The references contained within the SECNAV INST 3501.1 definitions are part of the definition within that instruction and were left intact.

Assessment (CIP): (1) An assessment is an objective evaluation of the vulnerabilities associated with Joint Force Capabilities. (2) Objective determination of how critical the capability and supporting infrastructure is in supporting military operations that accomplish the National Military Strategy. Focus is Combatant Command OPLANs. (3) A process to characterize DOD infrastructures, their dependencies and interdependencies and subsequent linkages to commercial, foreign and host nation infrastructures.

Asset: Any military/private/commercial resource, relationship, instrument, installation, supply or system that in some combination is used in a military operational or support role. Assets are found at CONUS and OCONUS locations.

Asset Criticality: Measure of impact of asset that supports other assets, infrastructures, or operational plans.

Capability (COCOM/Joint Force): Military Capability – The ability to achieve a specific wartime objective (win a war or battle, destroy a target set). It includes four major components: force structure, modernization, readiness, and sustainability.

(a) Force structure – Numbers, size, and composition of the units that comprise our Defense forces; e.g., divisions, ships, airwings.

(b) Modernization – Technical sophistication of forces, units weapons systems, and equipment.

(c) Unit Readiness – The ability to provide capabilities required by the combatant commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed.

(d) Sustainability – The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materials, and consumables necessary to support military effort.

Critical Asset: (1) Asset which can be either a DOD or non-DOD military-related unit, organization, facility, installation, system, resource, equipment, instrument, which is identified as performing an essential service, function, or use in military operational plans or support to operational plans. (2) Any facility, equipment, service or resource considered essential to DOD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical Assets may be DOD assets or other government or private assets, domestic or foreign, whose disruption or loss would render DOD Critical Assets ineffective or otherwise seriously disrupt

DOD operations. Critical Assets include both traditional "physical" facilities or equipment, non-physical assets (such as software systems) or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).)

Critical Infrastructure: Those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DOD 8500.1 (NOTAL))

Critical Infrastructure Assurance Officer (CIAO): The CIAO is responsible for the protection of all of the department's critical infrastructures. The CIAO shall establish procedures for obtaining expedient and valid authority to allow vulnerability assessments to be performed on computer and physical systems. The Department of the Navy CIAO is the Department of the Navy Chief Information Officer, who was initially appointed by Under Secretary of the Navy Memorandum of 26 August 1999 (NOTAL). The DON CIAO chairs the DON Critical Infrastructure Protection Council.

Critical Infrastructure Protection: CIP is Mission Protection. CIP is the identification, assessment, and assurance of Cyber and Physical infrastructures that support mission critical capabilities and requirements, to include the political, economic, technological, and informational security environments essential to the execution of the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DOD 8500.1(NOTAL))

Denial of Service: A form of attack that reduces the availability of a resource. (NP V 1.0)

Destruction: A Condition when the ability of a critical infrastructure to provide its customers an expected upon level of products and services is negated. Typically a permanent condition. An infrastructure is considered destroyed when its level of performance is zero. (NP V 1.0)

DOD Installation: A facility subject to the custody, jurisdiction, or administration of any DOD Component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, or laboratories where a DOD Component has operational responsibility for facility security and defense. Examples are facilities where the military commander or other specified DOD official under provisions of DOD Directive 5200.8, 25 April 1991, has issued orders or regulations for protection and security. Both industrial assets and infrastructure assets, not owned by the Department of Defense, may exist within the boundaries of a military installation (DODD 5160.54)

Event (*): In the context of Consequence Management, an event is a hostile act, accident or natural disaster.

Exercise (*): A test or drill in which actions in the contingency plan are performed or simulated as though responding to an event. It is during the exercise that planners and participants can evaluate whether the planned activities and tasks properly address potential situations.

Force Protection: Security program designed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services,

and supported by intelligence, counterintelligence, and other security programs. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

Guidance: (1) Policy, direction, decision, or instruction having the effect of an order when issued by a higher echelon. (2) The entire process by which target intelligence information received by the guided missile is used to effect proper flight control to cause timely direction changes for effective target interception. (JP 1-02)

Hot Site (*): A fully equipped computer facility. A hot site contains the stand-by computer equipment, environmental systems, communications capabilities, and other equipment necessary to fully support a using organization's immediate data processing requirements in the event of an emergency or a disaster.

Impact Analysis (*): The process of identifying an organization's exposure to the sudden loss of selected business functions and/or the supporting resources (threats), and analyzing the potential disruptive impact of those exposures (risks) on key business functions and critical business operations.

Incident Command System (ICS): ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in domestic incident management activities. ICS is a component of the National Incident Management System under the auspices of the Dept of Homeland Security. See "National Incident Management System".

Indications and Warning: Indications are preparatory actions or preliminary infrastructure states that signify that an incident is likely, is planned, or is underway. An official warning would be issued by the responsible organization.

Information Assurance: (1) Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02) (2) Information operations that protecting key public and private elements of the national information infrastructure from exploitation, degradation, and denial of service. (Modified from NSTAC)

Information Security: Information Security is the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information Security includes these measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02)

Information System: The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02)

Infrastructure: The framework of inter-dependent networks and systems comprising identifiable industries, institutions, functions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole. (DODD 5160.54) (DOD Plan – Nov 98) (NP V 1.0) Bilateral Infrastructure – p. 58 JP 1-02, Common Infrastructure – p. 93 JP 1-02, National Infrastructure – p. 302 JP 1-02.

Infrastructure Indications and Warning: Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the National Infrastructure Protection Center (NIPC) in concert with existing DOD and national capabilities. (CIP Working Definition)(DOD Plan – Nov 98)

Infrastructure Protection: Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures. For instance, threat deterrence and vulnerability defense.

Interdependence: Dependence among elements or sites of different infrastructures, and therefore, effects of one infrastructure upon another. (DOD Plan – Nov 98) (NP V 1.0)

Interruption (*): Any event, whether anticipated or unanticipated which disrupts the normal course of operations at any location.

Metrics: An agreed upon measure of performance. (NP V 1.0)

Military Capability: See "Capability"

Mission Critical: Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). (NP V 1.0)

Mission Essential: Any function that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

Mitigation: Action taken to reduce or eliminate vulnerability of people or infrastructure to threats and their effects. (Joint Staff Definition used in coordinated response to Draft DOD 8500.1 (NOTAL))

Naval Integrated Vulnerability Assessment: An expert third party or peer review comprehensive CIP assessment instrument under DON CIAO coordination and leadership synthesizing several existing assessment protocols including Marine Corps or CNO Integrated Vulnerability Assessments for Anti-terrorism and Force Protection; Marine Corps Enterprise Network (MCEN) or Fleet Information Warfare Center (FIWC) assessments for computer network vulnerability; non-organic and other commercial infrastructure assessments performed by Joint Program Office – Special Technology Countermeasures (JPO-STC) or other; and a continuity of operations plans and preparedness assessment under appropriate Navy or Marine Corps community direction. The NIVA is performed cyclically in all Navy Regions or other major Navy concentration areas, and at major Marine Corps Installations. Also referred to as a Full Spectrum Integrated Vulnerability Assessment (FSIVA) within DoD.

National Incident Management System (NIMS): Managed by the Department of Homeland Security, The NIMS, represents a core set of doctrine, concepts, principle, terminology, and organizational processes to enable effective, efficient and collaborative incident management at all levels. NIMS is not an operational incident management or resource allocation plan. See "Incident Command System".

Network: Information system implemented with a collection of interconnected nodes. (NP V 1.0)

Off-Site Storage (*): The process of storing vital records in a facility that is physically remote from the normal site. Usually this facility is environmentally protected for proper care and storage of magnetic media, microfilm, and paper.

Operational Impact: Impact of critical assets and OPLANS on other military operations (mobilization, deployment, force projections, etc.)

Operational Impact Analysis: The relationship between military plans and operations and critical assets established through the development of operational dependency matrices and application of operations research methodologies.

Operations Security: The process denying to potential adversaries information about capabilities and/or intentions by identifying, controlling and protecting generally unclassified evidence of the planning and execution of sensitive activities. (NIS)

Physical Security: (1) That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. See also Communications Security, Protective Security, Security. (JP 1-02, p.343) (2) Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks, e.g., through the use of conventional or unconventional weapons. (NP V 1.0)

Reconstitution: Refers to actions required to rebuild or restore an aspect or portion of an infrastructure after it has been degraded. Owner/operator directed restoration of critical assets and/or infrastructure. (DOD Plan – Nov 98)

Recovery (*): Those long-term activities and programs which are designed to be implemented beyond the initial crisis period of an emergency or disaster in order to return all systems to normal status or to reconstitute those systems to a new condition that is less vulnerable.

Reliability: The capability of a computer, or information or telecommunications system to perform consistently and precisely, according to its specifications and design requirements, and to do so with high confidence. (NP V 1.0)

Remediation: Those precautionary actions taken before undesirable events occur to improve known deficiencies and weaknesses that could cause an outage or compromise a defense infrastructure sector or critical asset. Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc.,

of critical assets and/or infrastructures, e.g., emergency planning for load shedding, graceful degradation, and priority restoration; increased awareness, training, and education; changes in business practices or operating procedures, asset hardening or design improvements, and system-level changes such as physical diversity, deception, redundancy, and back-ups. (NP V 1.0) Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc. of critical assets and/or infrastructures, e.g., emergency planning for load shedding, graceful degradation and priority restoration; increased awareness, training and education; changes in business practices or operating procedures, asset hardening or design improvements, and system level changes such as physical diversity, deception, redundancy and backups. (CIP Working Definition). (DOD Plan – Nov 98)

Response: Response refers to those activities undertaken to eliminate the cause or source of an event. It also includes emergency measures from dedicated third parties such as medical, police, and fire and rescue (Public Safety). Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident. (NP V 1.0)

Restoration (*): The act of returning a piece of equipment or some other resource to operational status. Commercial service companies provide a restoration service with staff skilled in restoring sensitive equipment or large facilities. Such vendors often work with insurance companies and may restore equipment for a fee or may purchase damaged equipment with the intent of restoring the equipment and re-marketing the product.

Risk: The probability that a particular threat will exploit a particular vulnerability of the system (NSA, NCSC Glossary Oct 88.) The probability that a particular critical infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation. (NP V 1.0)

Risk Analysis or Risk Assessment: The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk Analysis is part of Risk Management (NSA, NCSC Glossary Oct 88) produced from the combination of Threat and Vulnerability Assessments characterized by analyzing the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities. (NP V 1.0)

Risk Management: The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review (NSA, NCSC Glossary, Oct 88.) The deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, characterized by identifying, measuring and controlling risks to a level commensurate with an assigned value. (NP V 1.0)

Threat: A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and malicious intent of debilitating the defense or economic security of the United States. A threat may be an individual, organization, or nation. (NP V 1.0)

Threat Analysis: A continual process of compiling and examining all available information concerning potential conventional and asymmetric force activities by groups which would target a asset, facility, node, capability, or infrastructure. A threat analysis will review the factors of a hostile groups' existence, capability,

intentions, history and targeting as well as the security environment within which the friendly forces operate. Threat analysis is an essential step in identifying probability of conventional/asymmetric attack and results in a threat assessment.

Tier Definitions: As determined by the Geographic Combatant Commanders, Tier I - Warfighter suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.

Tier II - Sector or element suffers strategic functional failure, but warfighter strategic mission is accomplished.

Tier III - Individual element failures, but no debilitating strategic mission or core function impacts occur.

Tier IV - Everything else.

Vital Records (*): Records or documents, regardless of media (paper, microfilm, audio or video tape, computer disks, etc.) which, if damaged or destroyed, would disrupt business operations and information flows and cause considerable inconvenience and require replacement or recreation at considerable expense.

Vulnerability: (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system which cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in a unnatural (manmade) hostile environment. (3) In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)
A characteristic of a critical infrastructure design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat. (NP V 1.0)

Vulnerability Assessment: Assessment of probability that events will occur using scenario-driven vulnerability index. Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation. (NP V 1.0)

Warm Site (*): An alternate recovery facility partially equipped with hardware, communications, power, and environmental support equipment.

APPENDIX I: CONSEQUENCE MANAGEMENT READING & REFERENCE LIST

Appendix I: Consequence Management Reading & Reference List

GENERAL

Federal Preparedness Circular -65: *Federal Executive Branch Continuity Of Operations (COOP),* 50 pages, dated June 15, 2004.

State and Local Guide (SLG) 101: *Guide for All-Hazard Emergency Operations Planning*, 279 pages, dated September 1996.

Executive Order (EO) 12148, *Federal Emergency Management*, dated July 20, 1979, as amended.

Homeland Security Presidential Directive # 7, *Critical Infrastructure Identification, Prioritization, and Protection,* dated December 17, 2003.

Homeland Security Presidential Directive # 8, *National Preparedness*, dated December 17, 2003.

Presidential Decision Directive 56, *Managing Complex Contingency Operations*, May 1997.

Presidential Decision Directive 63, *Critical Infrastructure Protection (CIP)*, dated May 22, 1998.

Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998 (Highside document).

Title 36 CFR, Part 1236, *Management of Vital Records*, revised as of July 1, 2000.

Federal Emergency Management Agency. *Objectives for Local Emergency Management*, CPG 1-5. Washington, DC: FEMA, 1984.

Federal Emergency Management Agency. *Are You Ready? Your Guide to Disaster Preparedness*, H-34. Washington, DC: FEMA, 1993.

FEMA, *Disaster Mitigation Guide for Business and Industry*, FEMA-190. Washington, DC: FEMA, 1990.

FEMA. *Emergency Management Guide for Business and Industry*, FEMA-141. Washington, DC: FEMA, 1993.

DoD Directive 3020.26, *Continuity of Operations (COOP) Policy and Planning*, 8 pages, dated May 26, 1995

DoD Directive 3020.36, *Assignment of National Security Emergency Preparedness (NSEP) Responsibilities to DoD Components,* 27 pages, dated November 2, 1988 (Administrative Reissue w/ Change 1, March 12, 1993)

DoD Directive 3025.1, *Military Support to Civil Authorities*, 15 Jan 1993

DoD Directive 3025.1M, *DOD Manual for Civil Emergencies*, June 1994

DoD Directive 3025.12, *Military Assistance for Civil Disturbances*, 4 Feb 1994

DoD Directive 3025.15, *Military Assistance to Civil Authorities (MACA)*, 18 Feb 1998

DoD Directive 5160.4, *Critical Asset Assurance Program (CAAP),* 20 Jan 1998

DoD Directive 5525.5, *Cooperation with Civilian Law Enforcement Officials*, 17 Jan 1986, reissued w/Change 1, 20 Dec 1989

Office of Homeland Security, "*National Strategy For Homeland Security*," 90 pages, July 2002

The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* February 2003.

GOVERNMENT'S RESPONSIBILITY FOR EMERGENCY MANAGEMENT

National Governors' Association. *A Governor's Guide to Emergency Management. (Volume One - Natural Disasters)* Washington, DC: NGA, 2001

National Governors' Association. *A Governor's Guide to Emergency Management. (Volume Two - Homeland Security)* Washington, DC: NGA, 2002

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended. (The Stafford Act sets out the parameters of the federal response to major disasters as declared by the President.)

COMPREHENSIVE EMERGENCY MANAGEMENT

National Governors' Association. *1978 Emergency Preparedness Project: Final Report*. Washington, DC: NGA, 1978.

Drabek, T.E., and G.J. Hoetmer, eds. *Emergency Management: Principles and Practice for Local Government*. Washington, DC: ICMA, 1991.

FEMA. *Fire and Emergency Services Preparedness Guide for the Homeland Security Advisory System* First Edition - January 2004

GENERAL PROCESS

Drabek, T.E., and G.J. Hoetmer, eds. *Emergency Management: Principles and Practice for Local Government*. Washington, DC: ICMA, 1991. See especially Chapters 3, 4, and 7.

National Fire Protection Association 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs,* NFPA 1600. Quincy, MA: NFPA, 2000 Edition

Fleet Marine Forces Manual 3-1, Co*mmand and Staff Action*," 498 pages, dated 21 May 1979

HAZARD ANALYSIS: GENERAL CONCEPTS AND PRINCIPLES

Burby, R.J. "The Technical Feasibility of Risk Analysis", Chapter 7 of *Sharing Environmental Risks: How to Control Governments' Losses in Natural Disasters*. Boulder, CO: Westview Press, 1991. pp. 129-153.

Cheok, M.C., et al. *Development of a Methodology for Comprehensive Hazard Analysis - A Feasibility Study*, report prepared for FEMA. Gaithersburg, MD: NUS Corporation, 1985.

Council of State Governments. *The States and Natural Hazards*. Lexington, KY: 1979.

Fischhoff, B., et al. *Acceptable Risk*. Cambridge: Cambridge University Press, 1981.

Kates, R.W., et al., eds. *Perilous Progress: Managing the Hazards of Technology*. Boulder, CO: Westview Press, 1985.

Mitchell, J.K. "Human Dimensions of Environmental Hazards: Complexity Disparity, and the Search for Guidance", Chapter 6 of A. Kirby, ed.,

Nothing to Fear: Risks and Hazards in American Society. Tucson: University of Arizona Press, 1990.

National Fire Protection Association. *Recommended Practice for Disaster Management*, NFPA 1600. Quincy, MA: NFPA, 1995. See the Appendix.

Palm, R.I. *Natural Hazards: An Integrative Framework for Research and Planning*. Baltimore: Johns Hopkins University Press, 1990.

EMERGENCY OPERATIONS PLAN FORMAT

Daines, G.E. "Planning, Training, and Exercising", Chapter 6 of T.E. Drabek and G.J. Hoetmer, eds., *Emergency Management: Principles and Practice for Local Government*. Washington, DC: ICMA, 1991. pp. 161-200.

DIRECTION AND CONTROL

Federal Emergency Management Agency. *Emergency Operating Centers Handbook*, CPG 1-20. Washington, DC: FEMA, 1984.

FEMA. *Exemplary Practices in Emergency Management: The California FIRESCOPE Program*, FEMA-117. Emmitsburg, MD: NETC/EMI, 1987.

FEMA. *The Incident Command System*, NFA-ICS-SM. Emmitsburg, MD: NETC/NFA, 1989.

FEMA. *Incident Command System (ICS) and Emergency Operating Center (EOC) Interface*, Curriculum Advisory Committee Report. Emmitsburg, MD: NETC/EMI, 1991.

FEMA *Overview of the Incident Command System*, SM-305.7. Emmitsburg, MD: NETC/EMI, 1992.

FEMA. *Guidance for Radio Amateur Civil Emergency Service*, CPG 1-15. Washington, DC: FEMA, 1991.

Department of Homeland Security. *National Incident Management System*. March 1, 2004

EMERGENCY PUBLIC INFORMATION

The Federal Emergency Management Agency and the American Red Cross have prepared a number of brochures to give families information to protect themselves in emergencies and disasters. The three most popular are listed below; they are available through FEMA's Printing and Publications Branch or on FEMA's Web page (http://www.fema.gov):

- *Emergency Preparedness Checklist*, L-154
- *Your Family Disaster Plan*, L-191/ARC 4466
- *Your Family Disaster Supplies Kit*, L-189/ARC 4463

Holton, James L. *The Electronic Media and Disasters in the High-Tech Age*, FEMA 109. Emmitsburg, MD: NETC/EMI, 1985.

EVACUATION

Federal Emergency Management Agency. *Evacuation: An Assessment of Planning and Research*, RR-9. Washington, DC: FEMA, 1987.

FEMA. *Evacuation in Emergencies: An Annotated Guide to Research*. Washington, DC: FEMA, 1987.

FEMA. *Transportation Planning Guidelines for the Evacuation of Large Populations*, Comprehensive (or Contingency) Planning Guide (CPG) 2-15. Washington, DC: FEMA, 1984.

RESOURCE MANAGEMENT

Federal Emergency Management Agency/National Donations Steering Committee, *Donations Management Guidance Manual*, January 1995.

General Services Administration. *The Management of Resource Crises at State, Municipal, and Community Levels: A Guide for Contingency Planning*. Washington, DC: GSA, 1976.

OVERVIEW OF VARIOUS HAZARDS

Council of State Governments. *The States and Natural Hazards*. Lexington, KY: CSG, 1979.

Federal Emergency Management Agency. *Disaster Operations: A Handbook for Local Governments*, CPG 1-6. Washington, DC: FEMA, 1981.

FEMA. *Principal Threats Facing Communities and Local Emergency Management Coordinators*, FEMA-191. Washington, DC: FEMA, 1992.

FEMA. *Risks and Hazards - A State by State Guide*, FEMA-196. Washington, DC: FEMA, 1990.

EARTHQUAKE

Federal Emergency Management Agency. *Comprehensive Earthquake Preparedness Planning Guidelines: County*, FEMA-72. Washington, DC: FEMA, 1985.

FEMA. *Comprehensive Earthquake Preparedness Planning Guidelines: Large City*, FEMA-146. Washington, DC: FEMA, 1987.

FEMA. *Estimating Losses from Future Earthquakes*, FEMA-177. Washington, DC: FEMA, 1989.

FEMA. *State and Local Earthquake Hazards Reduction: Implementation of FEMA Funding and Support*, CPG 2-18. Washington, DC: FEMA, 1985.

FLOODING AND DAM FAILURE

Federal Emergency Management Agency. *Emergency Action Planning Guidelines for Dams*, FEMA-64. Washington, DC: FEMA, 1985.

FEMA *Federal Guidelines for Dam Safety*, FEMA-93. Washington, DC: FEMA, 1979.

FEMA. *Guide to Flood Insurance Rate Maps*, FIA-14. Washington, DC: FEMA, 1988.

FEMA *How to Read Flood Hazard Boundary Maps*, FIA-3. Washington, DC: FEMA, 1981.

FEMA. *Model State Dam Safety Program*, FEMA-123. Washington, DC: FEMA, 1987.

FEMA *National Dam Safety Program for State and Local Officials*, CPG 1-39. Washington, DC: FEMA, 1988.

FEMA. *Reducing Losses in High Risk Flood Hazard Areas: A Guidebook for Local Officials*, FEMA-116. Washington, DC: FEMA, 1987.

HAZARDOUS MATERIALS

Federal Emergency Management Agency. *Federal Radiological Emergency Response Plan (FRERP); Operational Plan; Notice.*. In: *Federal Register*, Vol. 61, No. 90, May 8, 1996.

FEMA. *Federal Radiological Emergency Response Plan (FRERP); Operational Plan; Correction.* In: *Federal Register*, Vol. 61, No. 109, June 5, 1996.

FEMA. *Guidance for Developing State, Tribal, and Local Radiological Emergency Response Planning and Preparedness for Transportation Accidents*, FEMA-REP-5, Rev. 1. Washington, DC: FEMA, 1992.

FEMA. *Guidelines for Public Sector Hazardous Materials Training: First Public Edition.*. Emmitsburg, MD: NETC/EMI, 1994. Developed under an agreement with the U.S. Department of Transportation and in coordination with other interested parties.

FEMA. *Preparedness for Hazardous Materials Emergencies in Railyards: Guidance for Railroads and Adjacent Communities*, FEMA-218. Washington, DC: FEMA, 1991.

FEMA, U.S. Department of Transportation, and Environmental Protection Agency. *Handbook of Chemical Analysis Procedures*. Washington, DC: FEMA, 1989.

National Response Team. *Hazardous Materials Emergency Planning Guide*, NRT-1. Washington, DC: NRT, 1987.

National Response Team. *Criteria for Review of Hazardous Materials Emergency Plans*, NRT-1A. Washington, DC: NRT, 1988.

U.S. Congress, Office of Technology Assessment. *Transportation of Hazardous Materials*, OTA-SET-304. Washington, DC: OTA, 1986.

U.S. Department of Energy. *Transporting Radioactive Material... Answers to Your Questions*, DOE/DP-0064. Washington, DC: DOE, 1989.

U.S. Department of Labor, Occupational Safety and Health Administration. *29 CFR Part 1910: Hazardous Waste Operations and Emergency Response; Final Rule*. In: *Federal Register*, Vol. 54, No. 42, March 6, 1989.

U.S. Department of Transportation. *Guidance for Conducting Hazardous Materials Flow Surveys*, DOT-VNTSC-RSPA-94-2. Washington, DC: US DOT, 1995.

DOT Transport Canada, Secretariat of Transport and Communications (Mexico). *1996 North American Emergency Response Guidebook*, NAERG96.

U.S. Environmental Protection Agency. *40 CFR Parts 9 and 300: National Oil and Hazardous Substances Pollution Contingency Plan; FinalRule.* In: *Federal Register*, Vol. 59, No. 178, September 15, 1994.

EPA. *Chemicals in Your Community: A Guide to the Emergency Planning and Community Right-to-Know Act*, EPA-550-K-93-003. Washington, DC: US EPA, 1988.

EPA. *A Review of Federal Authorities for Hazardous Materials Accident Safety,* EPA-550-R-93-002. Washington, DC: US EPA, 1993.

EPA. *SARA Title III Fact Sheet*, EPA-550-F-93-002. Washington, DC: US EPA, 1993.

EPA. U.S. Department of Transportation, and Federal Emergency Management Agency. *Technical Guidance for Hazards Analysis: Emergency Planning for Extremely Hazardous Substances*. Washington, DC: US EPA, 1987.

U.S. House of Representatives, Committee on Public Works and Transportation, Subcommittee on Surface Transport. *Transportation of Hazardous Materials - Hearings*, 101-52. Washington, DC: GPO, 1989.

HURRICANE

Federal Emergency Management Agency. *Guide to Hurricane Preparedness Planning for State and Local Officials*, CPG 2-16. Washington, DC: 1984.

LETHAL UNITARY CHEMICAL AGENTS AND MUNITIONS

Federal Emergency Management Agency and U.S. Department of the Army. *Planning Guidance for the Chemical Stockpile Emergency Preparedness Program*. Washington, DC: FEMA, 1994.

NUCLEAR CONFLICT

Federal Emergency Management Agency. *Life Support Operations in Shelters*, CPG 2-20. Washington, DC: FEMA, 1988.

FEMA. *Nuclear Attack Environment Handbook*, H-21. Washington, DC: FEMA, 1990.

FEMA. *Radiation Safety in Shelters*, CPG 2-6.4. Washington, DC: FEMA, 1983.

National Security Council. *The National Security Strategy of the United States of America - Report*. Washington, DC: NSC, February 25, 1994.

Center for Strategic and International Studies. "*Combating Chemical, Biological, Radiological and Nuclear Terrorism: A Comprehensive Strategy*." Frank J. Cilluffo, Sharon L. Cardash, and Gordon N. Lederman. December 2000

NUCLEAR POWER PLANT ACCIDENTS

Federal Emergency Management Agency. *Criteria for Preparation and Evaluation of Radiological Emergency Plans and Preparedness In Support of Nuclear Power Plants*, NUREG-0654/FEMA REP-1, Rev. 1. Washington, DC: FEMA, 1987.

FEMA. *Federal Radiological Emergency Response Plan (FRERP); Operational Plan; Notice*. In: *Federal Register*, Vol. 61, No. 90, May 8, 1996.

FEMA. *Federal Radiological Emergency Response Plan (FRERP); Operational Plan; Correction*. In: *Federal Register*, Vol. 61, No. 109, June 5, 1996.

U.S. Environmental Protection Agency. *Manual of Protective Action Guides and Protective Actions for Nuclear Incidents*, EPA 400-R-92-001. Washington, DC: US EPA, 1991.

LINKING FEDERAL AND STATE EMERGENCY RESPONSE OPERATIONS

Federal Emergency Management Agency. *The Federal Response Plan*, FEMA-229. Washington, DC: FEMA, 1992.

Office of Homeland Security, *National Strategy for Homeland Security*, July 2002

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended. (The Stafford Act sets out the parameters of the federal response to major disasters as declared by the President.)

ANTITERRORISM AND FORCE PROTECTION

United States Government Interagency Domestic Terrorism Concept of Operations Plan, 36 pages, dated January 2001

GAO-03-165, "*Combating Terrorism*" Raymond J. Decker, Director, Defense Capabilities and Management. Dated May 23, 2003

Presidential Decision Directive (PDD) 39 "*U.S. Policy on Counterterrorism*," June 21, 1995

PDD 62 "*Protection Against Unconventional Threats to the Homeland and Americans Overseas*," May 22, 1998. This PDD reinforced the mission of the agencies charged with roles in combating terrorism. It also codified and clarified their activities in the wide range of counterterrorism programs, from apprehension and prosecution of terrorists to increasing transportation security, to enhancing response capabilities and protecting computer-based systems. PDD 62 also established the Office of the National Coordinator for Security,

Infrastructure Protection and Counter-Terrorism. The National Coordinator oversees the broad variety of relevant policies and programs, including such areas as counterterrorism, protection of critical infrastructure, and preparedness and consequence management for (WMD). Mitigation of the effects of a WMD attack is where HHS and CDC would become active, especially if an attack(s) involved lethal biological agents. Additionally, PDD 62 led to the creation of the National Domestic Preparedness Office (NDPO). Under the auspices of the Department of Justice and FBI, the NDPO coordinates all federal efforts, including those of DoD, FEMA, HHS, DoE, and the EPA, to assist state and local first responders with planning, training, equipment, and exercise necessary to respond to a conventional or non-conventional weapon of mass destruction (WMD) incident.

INTERNATIONAL, CROSS-INDUSTRY STANDARDS

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17799: 2000 *Information Technology—Code of Practice for Information Security Management*, an international version of British Standard 7799-1:1999, was published in December 2000. It contains 10 major sections, one of which is business continuity management (Section 11); however, parts of Physical and Environmental Security (7), Asset Classification and Control (5) and Security Policy (3) warrant reading. Section 11 of ISO 17799 is devoted solely to business continuity and disaster recovery.

ISO/IEC Technical Report (TR) 13335, *Guidelines for the Management of IT Security* (*GMITS*), 13335-2: *Managing and Planning IT Security*, contains requirements for procedural security, including business continuity.

ISO 9002 quality assurance model applies to organizations that produce, install and service products. It implies industry standards for IT Security and the broader subject of general product security, including continuity planning for IT systems—both as products themselves and as environmental support—and all other aspects of business operations (physical, environmental, personnel) whose disruption would affect product security.

NIST Special Publications (SP) 800 Series (parts 3, 4, 12, 14, 16 and 18) require contingency, disaster recovery and continuity of operations plans.

INDUSTRY-SPECIFIC STANDARDS AND REGULATIONS

U.S. FEDERAL GOVERNMENT

Government agencies with essential missions at federal, state and local levels have always had continuity plans. The COOP directives produced by the Office of Management and Budget (OMB) and the President of the United States outline the objectives of business continuity planning for all federal departments and agencies. Examples are as follows:

OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," published in 1993, ensures that appropriate business continuity plans were put in place for all federal general-purpose systems and major applications, which include the mission-critical applications identified under the Y2K program.

Executive Order 12656 (Section 202) of 1988 requires the head of each federal department and agency to ensure the continuity of essential functions in national security emergencies by providing for safekeeping of essential resources, facilities, and records and establishment of emergency operating capabilities.

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING AND MANAGEMENT: TECHNOLOGY OVERVIEW

FINANCE

The Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, in its new version issued 18 April 2003, holds legal weight—unlike the original version, which provided regulatory guidance. Under this version, the Office of the Comptroller of the Currency (OCC) will take action against banks that fail to comply with the document requirements for disaster recovery by the U.S. financial system. The new version gives firms more latitude to determine the distance between their live and recovery sites, an issue that drew much negative reaction during the comment period for the original plan.

Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook 2003 update is under revision into separate booklets that will eventually replace the original Handbook. One booklet guides examiners evaluating financial institution and service provider risk management processes for availability of critical financial services. The booklet for supervision of technology service providers guides examination of services performed for financial institutions. It emphasizes that the ultimate responsibility resides with an institution's management and board of directors to ensure outsourced activities are conducted in a safe and sound manner, in compliance with related laws and regulations.

BASEL COMMITTEE ON BANKING SUPERVISION, BANK FOR INTERNATIONAL SETTLEMENTS (BIS),

Publication 82—Risk Management for Electronic Banking, Principle 13: The Third Consultative Paper (published 28 April 2003) contains the final modifications to its proposal for a new capital adequacy framework. The new capital adequacy framework places new demands on BC and DR for financial services. The BIS's September 2002 update of its "Sound Practices for the Management and Supervision of Operational Risk" provides a framework for effective management and supervision of operational risk by banks and supervisory

authorities when evaluating operational risk management policies and practices. The original May 2001 publication states that banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services. Expected completion date is fourth quarter of 2003, with implementation effective in member countries by year-end 2006.

The U.S. Sarbanes-Oxley Act (SOX), a new rule issued by the SEC on 31 October 2002, responds to revelations of executive and auditing malfeasance scandals by expanding the requirements for corporate reporting for auditors, managers and audit committees. Auditing firms, for example, must keep for at least seven years *every* document that influences its report about a client, including such bits as a CEO's e-mail or a sticky note with some figures on it. Evolving legal interpretations of the rules imply that, pragmatically, every public (and possibly private) company must keep these records too in order to avoid liability in an unforeseeable investigation. The preservation of the systems that process and store these records takes on increased importance.

Gramm-Leach-Bliley Act of 1999 (compliance deadline 1 July 2001), Section 501(b) Financial Institutions Safeguards, requires that the agencies described in Section 505(a) establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards for the security and confidentiality of customer records and information.

SAS70 Reports (1993) in accord with a statement on Auditing Standards Number 70 issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA)—review the processing of transactions by service organizations, such as electronic data processing (EDP) centers and banks. SAS70 reports must be performed by certified external auditors, who examine general computer controls, qualified service providers, participant eligibility, and claim system application controls and review the findings with management.

The Expedited Funds Availability (EFA) Act, enacted by the U.S. Controller of Currency on 1 January 1989, requires federally chartered financial institutions to have a demonstrable business continuity plan to ensure prompt availability of funds. Regulation CC (12 C.F.R. Part 229) from Board of Governors of the Federal Reserve System implements the EFA. The regulation also establishes rules for the prompt collection and return of unpaid checks. Regulation CC contains three subparts. Subpart A defines terms and describes administrative enforcement. Subpart B specifies availability time frames within which banks must make funds available for withdrawal. Subpart C establishes the rules to ensure the speedy return of checks, the responsibilities of paying

and returning banks, authorization of direct returns, notification of nonpayment of large-dollar returns by the paying bank, check endorsement standards and other charges related to the check collection system.

HEALTH

Health Insurance Portability and Accountability Act (HIPAA) In April 2003, the U.S. HIPAA Privacy Rule to protect patients' health information went into effect. The Privacy Rule affects all forms of protected information, including oral and hand-written communications, as well as the electronic forms covered in the original 1996 Act, which requires healthcare plans, providers and clearinghouses to adopt standardized electronic claims and payment systems. Noncompliance fines start at $100 for failure to meet a standard, but range up to $250,000 and 10 years' imprisonment for the wrongful use or disclosure of individual health information for commercial advantage, personal gain and the like. Also, accreditation agencies, such as the Joint Commission on Accreditation of Health Care Organizations (JCAHO), inspect for compliance during their accreditation process. In February 2003, the Department of HHS published the HIPAA Security Rule, which becomes effective 21 April 2005. The Security Rule applies only to patient-identified electronic Protected Health Information (PHI). The electronic signature standard has been removed, although HHS states that it will be published later as a separate regulation. Section 164.306(a) of the Security Rule states four general requirements for covered entities, from which many specific standards and implementation specifications derive. Some of the implementation specifications associated with the standards in the Security Rule are required, and the others are addressable.

Food and Drug Administration's (FDA's) Code of Federal Regulations (CFR), Title XXI, 1999 The rule establishes the requirements for electronic records and electronic signatures to be considered trustworthy, reliable and essentially equivalent to paper records and handwritten signatures executed on paper. It applies to any electronic-format records covered by FDA regulations, including records that are required to be maintained whether or not they are submitted to the FDA.

U.S. Department Of Health And Human Services, Centers for Disease Control and Prevention. The Public Health Response To Biological And Chemical Terrorism, *Interim Planning Guidance For State Public Health Officials.* July 2001

U.S. Department Of Health And Human Services, Centers for Disease Control and Prevention. *Interim Smallpox Response Plan and Guidelines*, November 26, 2001 (Updated March 21, 2003). This 10-page document outlines how health officials all over the country should react in the event of a smallpox outbreak.

UTILITIES

The Telecommunications Act of 1996, Section 256, "**Coordination for Interconnection,**" requires the FCC to establish procedures to oversee coordinated network planning by telecommunications carriers and other providers of telecommunications service. It also permits the FCC to participate in the development of public network interconnectivity standards by appropriate industry standards-setting bodies. The act recognizes the need for disaster recovery plans, but also acknowledges the existence of inadequate testing because of the rapid deployment of new technologies.

INFORMATION TECHNOLOGY

The National Institute of Standards and Technology (NIST) Special Publication 800-34, ***Contingency Planning Guide for Information Technology Systems,*** Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. 107 pages, dated June 2002. This document defines detailed recommendations from the NIST, a division of the Technology Administration of the U.S. Department of Commerce. It joins the NIST Special Publications (SP) 800 series (parts 3, 4, 12, 14, 16, 18 and now 34) requiring contingency, disaster recovery and continuity of operations plans. While the document serves as official guidance only to U.S. government agencies, IT professionals in all industries pay due attention to such publications. SP 800-34 asserts that successful contingency planning management must ensure (1) understanding of the IT Contingency Planning Process and its place within the overall Business Continuity Plan process; (2) development or re-examination of contingency policy and planning process and application of the elements of the planning cycle, including preliminary planning, business impact analysis, alternate site selection and recovery strategies; and (3) development or re-examination of IT contingency planning policies and plans with emphasis on maintenance, training and exercising the contingency plan.

AFTER-ACTION REPORTS, REVIEW OF PLANS, ARTICLES, ETC.

Department of Homeland Security Releases Summary Conclusions From National Exercise (TOPOFF2), 3 pages. December 19, 2003

Commonwealth of Virginia. *Emergency Operations Plan, Volume 5, "Hurricane Emergency Response*," 113 pages. Virginia Department of Emergency Management, August 2001

Fourth Annual Report To The President And The Congress Of The Advisory Panel To Assess Domestic Response

Capabilities For Terrorism Involving Weapons Of Mass Destruction, Implementing The National Strategy. James S. Gilmore, III, Chairman, 348 pages, 15 December 2002

Review of *Navy Marine Corps Intranet Disaster Preparedness Plan* (December 2001 - January 2002)

Arlington County *After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon* (undated - 2002)

Review of *District of Columbia Disaster Preparedness Plan*, January 2002

GAO Report. *CONTINUITY OF OPERATIONS Improved Planning Needed to Ensure Delivery of Essential Government Services,* February 2004.

GAO Report. *POTENTIAL TERRORIST ATTACKS Additional Actions Needed to Better Prepare Critical Financial Market Participants*, February 2003.

GAO Report. *BUILDING SECURITY: Security Responsibilities for Federally Owned and Leased Facilities*, October 2002.

DON CMPG 2.0

DEPARTMENT OF THE NAVY

CRITICAL INFRASTRUCTURE ASSURANCE OFFICER

1000 NAVY PENTAGON

WASHINGTON, DC 20350-1000

www.doncio.navy.mil