2006-09

Emergency preparedness and response systems

Alvarez, Maria Doris

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/2683

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMERGENCY PREPAREDNESS AND RESPONSE SYSTEMS

by

Maria Doris Alvarez

September 2006

Thesis Advisor:	Alex Bordertsky
Second Reader:	Dan Dolk

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE: Emergency Preparedness and Response Systems **6. AUTHOR(S)** Maria Doris Alvarez	**5. FUNDING NUMBERS**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The objective of this thesis is to review and analyze the current Command and Control communications used by the New Jersey Department of Health and Senior Services and provide best business practices of Emergency Preparedness and Response Systems capable of responding to all public health emergencies, act of terrorism and mass casualty incidents.

Natural and man-made disasters, such as earthquakes, floods, plane crashes, high-rise building collapses, or major nuclear facility malfunctions, pose an ever-present danger challenge to public emergency services. In order to manage such disasters in a rapid and highly efficient and coordinated manner, the optimal provisions of information concerning any crisis situation is an essential pre-requisite. Local Police, Fire departments, Public Health Department, Civil Defense, Military and other emergency response organizations must react efficiently yet individually but most importantly, in a coordinated manner. These results in the necessity for both intra and inter organization coordination at several hierarchy levels. Since coordination requires current information, such information must be communicated within and between organizations in real-time, the need arises for an integrated communication and information system solely designated or disaster management that provides processing of relevant efficient, reliable and secure exchange of information.

14. SUBJECT TERMS Emergency Response, Disaster Response Plan, Terrorism	**15. NUMBER OF PAGES** 173
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

EMERGENCY PREPAREDNESS AND RESPONSE SYSTEMS

Maria D. Alvarez
Lieutenant, United States Navy
M.B.A., Regent University, 1999
M.S., California State University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Maria Doris Alvarez

Approved by: Alex Bordetsky
Thesis Advisor

Dan Dolk
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The objective of this thesis is to review and analyze the current Command and Control communications used by the New Jersey Department of Health and Senior Services and provide best business practices of Emergency Preparedness and Response Systems capable of responding to all public health emergencies, act of terrorism and mass casualty incidents.

Natural and man-made disasters, such as earthquakes, floods, plane crashes, high-rise building collapses, or major nuclear facility malfunctions, pose an ever-present danger challenge to public emergency services. In order to manage such disasters in a rapid and highly efficient and coordinated manner, the optimal provisions of information concerning any crisis situation is an essential pre-requisite. Local Police, Fire departments, Public Health Department, Civil Defense, Military and other emergency response organizations must react efficiently yet individually but most importantly, in a coordinated manner. These results in the necessity for both intra and inter organization coordination at several hierarchy levels. Since coordination requires current information, such information must be communicated within and between organizations in real-time, the need arises for an integrated communication and information system solely designated or disaster management that provides processing of relevant efficient, reliable and secure exchange of information.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIDS Acquired Immune Deficiency Syndrome

BIDS Border Infectious Diseases Surveillance (CDC)
BPRP Bioterrorism Preparedness and Response Program (CDC)
BSERT Bioterrorism Surveillance and Epidemiologic Response Team (DISB)
BT Bioterrorism

CAHFSL California Animal Health and Food Safety Laboratory System (CDFA)
CHS California Center for Health Statistics
CCLHO California Conference of Local Health Officers
CD Communicable Disease
CDC Centers for Disease Control and Prevention
CDFA California Department of Food and Agriculture
CDFG California Department of Fish and Game
CELDAR California Electronic Laboratory Disease Alert and Reporting System
CISP California Influenza Surveillance Project

DCDC Division of Communicable Disease Control (NJDHSS)
DIS Disease Investigations Section (DISB)
DISB Disease Investigations and Surveillance Branch (DCDC)
DCDC DOD DCDC Duty Officer of the Day (NJDHSS)
DNC Democratic National Convention

EIP Emerging Infections Program
EISO Epidemic Intelligence Service Officer
ELR Electronic Laboratory Reporting
EMSA Emergency Medical Services Authority
Epi-X Epidemic Information Exchange
EPO Emergency Preparedness Office (NJDHSS)
ED Emergency Department
EEE Eastern Equine Encephalitis
EMS Emergency Medical Services
ER Emergency Room

FBI Federal Bureau of Investigation

GIS Geological Information System

HAN Health Alert Network
HIV Human Immunodeficiency Virus
HMO Health Maintenance Organization

ICP Infection Control Practitioner
ICU Intensive Care Unit
ILI Influenza Like Illness

LHD Local Health Department
LLNL Lawrence Livermore National Laboratory
LRN Laboratory Response Network

MDL Microbial Diseases Laboratory (DCDC)
MMRS Metropolitan Medical Response System (USPHS)

NEDSS National Electronic Disease Surveillance System
NETSS National Electronic Telecommunications Systems for Surveillance
NJDHSS New Jersey Department of Health and Senior Services
NJDHSS DO NJDHSS Duty Officer

OES Office of Emergency Services
OPA Office of Public Affairs

PIO Public Information Officer
POC Point of Contact
PPE Personal Protective Equipment

RHEACTS Rapid Health Electronic Alert, Communications and Training System
RRT San Diego Rapid Response Team

SLE St. Louis Encephalitis
SSS Surveillance and Statistics Section (DISB)

UCLA University of California, Los Angeles
UNEX Unexplained Illness and Death Project
USPHS United States Public Health Service

VBDS Vector-Borne Diseases Section (DISB)
VEE Venezuelan Equine Encephalitis
VHF Viral Hemorrhagic Fever
VPHS Veterinary Public Health Section (DISB)
VRDL Viral and Rickettsial Disease Laboratory (DCDC)

WEE Western Equine Encephalitis

ACKNOWLEDGMENTS

I would like to thank God for all His blessings and guidance of which I am eternally grateful. I would also like to take this opportunity to thank Professor Alex Bordetsky for his unwavering dedication and expert advice to this project. I would like to extend my thanks to Professor Glen Cook for his invaluable advice, patience and understanding.

I would also like to thank my husband who has helped me throughout my career in the Navy and was always there to help me with my goals but most of all for helping me get through the taught times and cheer me in the good times. I would like to extend my thanks to those of you who assisted me in completing this endeavor. Your willingness to assist me throughout this endeavor will never be forgotten. I am grateful for your patience, understanding, encouragement, and personal efforts afforded to me throughout my NPS experience and the development of this thesis. Thank you!!

Lew Esquibel
Alex Bordetsky
Dan Dolk
Glen Cook
Dan Boger
Gretchen Fenniger
Jim Martin

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

In many organizations, individuals must be brought into the same room in order to effectively collaborate. Also, complex responses are often managed only by voice communications, causing distortion of information passed from point to point and poor incident documentation. Some organizations try to pass information by facsimile machine, but find that method too slow and troublesome. Many metropolitan areas still use “un-sharable” acetate boards in operations centers to track status of the incident and resources as I experience during the California State wide exercise. In short, responders often feel left behind by the digital information revolution.

All Civilian Health Care activities (public or private) and Military Treatment Facilities (MTF's) are required to have a contingency plan and/or emergency plans. An Emergency plan comprises a structured collection of actions that must be followed to adequately respond to an anticipated set of scenarios.

The proposed research within this thesis evaluated Disaster Response Plans from Civilian and Military entities focusing on a general skeleton that will provide the New Jersey Department of Health and Senior Services (NJDHSS) or any other entity a guide/template to follow and be able to create their unique Disaster Response Plan (Chapter 2) to include guiding principles, and the life cycle of Incident Management Activities always ensuring the privacy of medical information. In addition as part of an Emergency Response System, I researched available technologies (Chapter 8) that will have most or all tools that are needed to respond to a disaster.

It is my conclusion that the Disaster Management Information System (DMIS) is the system of choice. DMIS solution has an interoperability platform and a set of basic tools. The interoperability backbone is one of the most important aspects of DMIS. It is the backbone that allows responders to acquire software that best suits their needs without having to worry about their neighbors buying the same software. The backbone enables information sharing among all systems that develop an automated program

interface to it. In addition the basic tools provide responders with the basic ability to describe an incident and request specific needs as described in appendix D.

I. INTRODUCTION

A. SITUATION ANALYSIS

Natural and man-made disasters, such as earthquakes, floods, plane crashes, high-rise building collapses, or major nuclear facility malfunctions, pose an ever-present danger challenge to public emergency services. In order to manage such disasters in a rapid and highly efficient and coordinated manner, the optimal provisions of information concerning any crisis situation is an essential pre-requisite. Local Police, Fire departments, Public Health Department, Civil Defense, Military and other emergency response organizations must react efficiently yet individually but most importantly, in a coordinated manner. These results in the necessity for both intra and inter organization coordination at several hierarchy levels. Since coordination requires current information, such information must be communicated within and between organizations in real-time, the need arises for an integrated communication and information system solely designated or disaster management that provides processing of relevant efficient, reliable and secure exchange of information.

Upon return from the planning meeting in March 2006, the New Jersey – NPS team took the responsibility of finalizing the Analysis of system and networking relationships for NJ Medical Response Command and Control architecture among other action items. Below is a diagram of the Response System C2 relationships analysis:

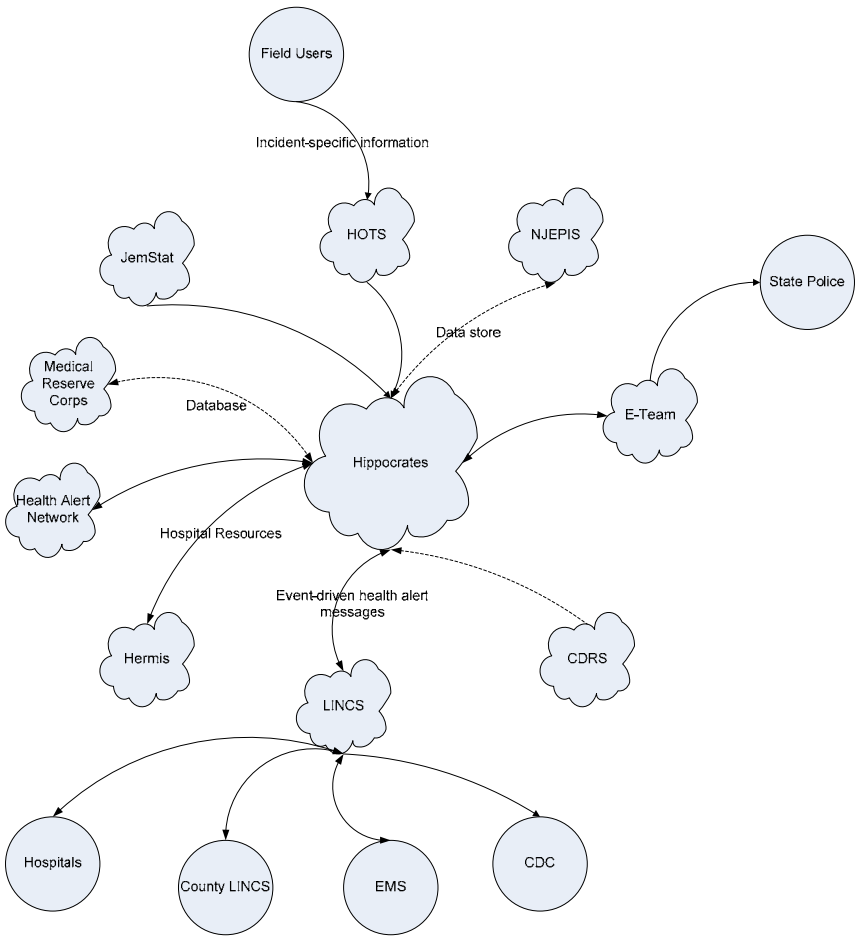


Figure 1. NJDHSS System Diagram (From: NPS Team Progress Report)

We reviewed the topology of information flows between major entities (people, organizations, and systems). Our perspective centered on Hippocrates as a central link or "dashboard" over all other systems. We then connected all other nodes to Hippocrates, and then branched out to origins of those systems' data.

The symbol convention used in this diagram distinguishes between systems (represented as clouds) and organizations (represented as circles). A line connects each pair of communicating entities, with the arrows showing the direction of information flow. Solid lines refer to existing system links, dashed lines refer to future planned links.

Hippocrates acts as the central hub for all information flows, pulling from and sometimes pushing to other systems within the state, and displaying that information to users as an overview of the total situational state. The network diagram below shows the physical and logical connections between the sites that host the NJLINCS portal:

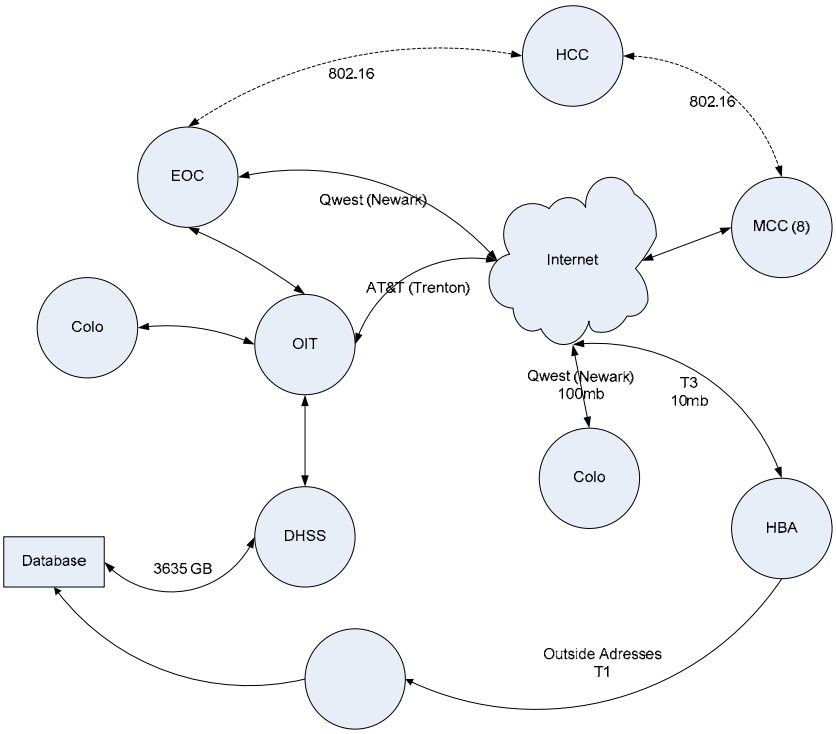


Figure 2. NJDHSS Network Diagram (From: NPS Team Progress Report)

The information flow diagram we developed to cover signaling in a potential influenza outbreak is also attached. All information flows begin when a sick person seeks treatment. This treatment is recorded in CDRS either by the school nurse (if a school student) or by the treating hospital or treatment facility. This is a weekly input for the school nurses, but event-driven input by the hospitals. Laboratory reports also are submitted to CDRS. Weekly, the hospitals fax aggregate data to NJLINCS. When appropriate, LINCS makes inputs to CDRS as well.

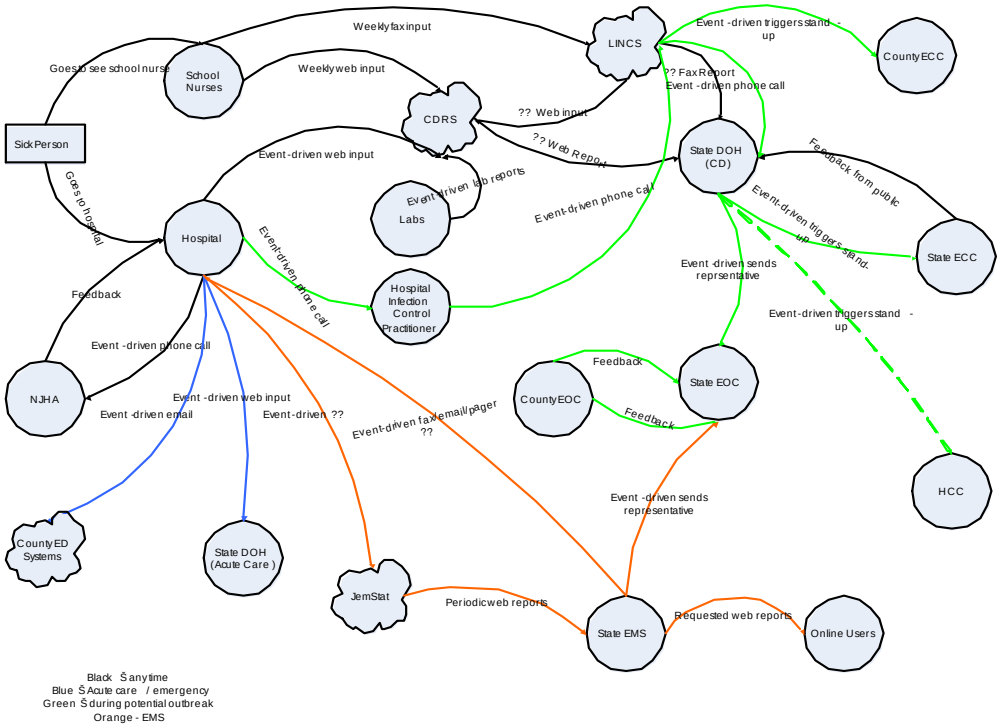


Figure 3. Information Flow Diagram (From: NPS Team Progress Report)

In the case that a hospital administrator or other responsible party believes an outbreak is occurring, many other information flows are triggered. Emails go to the County ED systems, EMS is alerted, JemStat receives the information, the Infection

Control Practitioner is alerted by the hospital, the State DOH&SS (Acute Care) is informed, and potentially NJLINCS informs the State DOH&SS (Communicable Diseases). If appropriate, at this point, the State DOH&SS stands up the ECC, as may County LINCS agencies. If the problem is worthy, the State may choose to establish State, County and Local EOCs to deal with the situation, in which case the DOH&SS sends representatives to the State EOC. (From: NPS Progress Report)

Unfortunately there are number of unanswered questions in the above diagrams and most of all the roles and responsibilities of each entity, method of information transfer is unknown, what rules are used to determine if an event triggers notification to higher authority, what do the information sinks do with the information they receive. Due to the numerous questions and the project being put on hold I am including examples that are currently used by the California's Health and Human Services Response Plan that can be used by the NJDHSS. Appendix A is a basic plan that should help to assist the

NJDHSS and its cities and towns in their preparedness activities to respond to an infectious disease emergency, such as an influenza pandemic or bioterrorism agent release, in order to minimize morbidity and mortality, and maintain health care and other essential community services during periods of high absenteeism due to illness. Appendix B is a guide for a Bioterrorism Surveillance and Epidemiologic Response Plan that is the product of collaborative efforts involving public health partners at the local, state, and federal levels. Appendix C is a list of the Center of Disease and Control (CDC) for Top Priority Bioterrorism Threat Agents.

The New Jersey Department of Health and Senior Services requested NPS to provide best business practices of Emergency Preparedness and Response Systems capable of responding to all public health emergencies, act of terrorism and mass casualty incidents as described in the Cooperative Research and Development Agreement below.

B. BACKGROUND

The New Jersey Department of Health and Senior Under authority of the U.S. Federal Technology Transfer Act of 1986 (Public Law 99-502, 20 October 1986, as amended), and the Naval Postgraduate School (NPS) have entered into a Cooperative Research and Development Agreement (CRADA).

The U.S. Federal Technology Transfer Act of 1986, as amended, provides for developing the expertise, capabilities, and technologies of U.S. Federal laboratories accessible to other Federal agencies; units of State or local governments, industrial organizations (including corporations, partnerships and limited partnerships, and industrial development organizations); public and private foundations; nonprofit organizations (including universities); or other persons in order to improve the economic, environmental, and social well-being of the United States by stimulating utilization of U.S. Federally funded technology developments and/or capabilities. NPS has extensive expertise, capabilities, and information in command and control infrastructures and, in accordance with the U.S. Federal Technology Transfer Act, desires to make this expertise and technology available for use in both the public and private sectors.

DHSS and NPS wish to explore the requirements for designing and implementing a command and control infrastructure for New Jersey's health emergency preparedness and response network. DHSS has the statutory authority under N.J.S.A 26:1A-15 to design and prototype health command centers (HCC), design and evaluate networking solutions for the DHSS medical rapid response team's communication with the command and control infrastructure of the State's Medical Coordination centers (MCC) and to explore the integration solutions for command center communication with legacy data bases at emergency preparedness and response, emergency medical services, special operations group sites, disaster medical assistance sites, and mass casualty response. DHSS finds it in the public interest to provide strategic and operational leadership and direction, coordination, provision of services, and assessment of activities to ensure state and local readiness, interagency/ multidisciplinary collaboration, preparedness for terrorism and other outbreaks of infectious disease, natural disasters, and other public health threats and emergencies (From CRADA documentation).

Complex and emerging 21st century hazardous threats demand a unified coordinated national approach to domestic incident management. The National Strategy for Homeland Security (Homeland Security Act of 2002) and Homeland Security Presidential Directive-5 (HSPD-5) Management of Domestic Incidents, establish clear objectives for a concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; minimize damage, and recover from attacks, major disasters, or other emergencies that occur. Achieving these objectives is challenging, requiring bold steps and adjustments to established structures, processes, and protocols.

An important initiative is the development and implementation of a National Response Plan (NRP), predicated on a new National Incident Management System (NIMS), that aligns the patchwork of Federal special-purpose incident management and emergency response plans into an effective and efficient structure. Together, the NRP and the NIMS (published March 1, 2004) integrate capabilities and resources of various governmental jurisdictions, incident management and emergency response disciplines, nongovernmental organizations (NGOs), and the private sector into one cohesive, coordinated, and seamless national framework for domestic incident management.

Consistent with the model provided in the NIMS, NRP can be partially or fully implemented in the context of a threat, anticipation of a significant event, or the response to a significant event. Selective implementation through the activation of one or more of the system's components allows maximum flexibility in meeting the unique operational and information-sharing requirements of the situation at hand and enabling effective interaction between various Federal and non-Federal entities. The NRP, employing NIMS, is an all-hazards plan that provides the structure and mechanisms for national level policy and operational coordination for domestic incident management.

C. OBJECTIVE

The objective of this thesis is research best business practice for Disaster Response Plan and available technologies that are "sharable" with other organizations. For the Disaster Response Plan we will take a Top-Down approach starting with NMIS Plan to the Regional level which the New Jersey DHSS position is located.

D. ORGANIZATION OF THESIS

Chapter I is the situational analysis, background and organization of the thesis. The New Jersey Department of Health and Senior Services requested NPS to provide best business practices of Emergency Preparedness and Response Systems capable of responding to all public health emergencies, act of terrorism and mass casualty incidents as described in the Cooperative Research and Development Agreement

Chapter II is an introduction to the Incident Command System (ICS). Incident Command System (ICS) is an organizational tool that can be thought of as both a requirement of public health and disaster response agencies and as an internal requirement for good emergency response management

Chapter III is the Organization of the New Jersey DHSS proposed plan. The plan is a general guideline that provides the region with a comprehensive approach to managing all domestic contingencies. When fully developed, the NJDHSSP should not be an umbrella for existing Regional incident management

plans; rather, it should build upon or incorporate what is best in the current plans of Regional, State, and local agencies, as well as those of private voluntary organizations, non-governmental organizations, and the private sector.

Chapter IV explains the several steps an Organization must follow to create a Disaster Response Plan; it includes functional areas, guidelines for a comprehensive plan and the plan elements.

Chapter V is the Assumptions and Consideration for a Disaster Response Plan. . In keeping with the requirements of HSPD-5, NJDHSS should prepare a single plan that is flexible enough to accommodate 'all hazards,' covering all of the disciplines required for conducting activities throughout the 'Life Cycle' of an incident. Under the NJDHSS, 'hazards' plan should refer to the full range of possible contingencies.

Chapter VI is the Life Cycle of Incident Management Activities and information security. The life cycle of activities is best described as containing five domains within which domestic incident management activities occur: awareness, prevention, preparedness, response, and recovery

Chapter VII in this chapter we move away from the Disaster Response plan to information systems and the Available Technologies. Throughout my research I identified various suitable technologies but only one technology 'stood out above the crowd'; is the Disaster Management Interoperability Services (DMIS). DMIS is not only compatible with other systems but it was also one of the systems identified by the U.S. government as 'the system of choice.'

Chapter VIII part of the thesis, I research and found what Navy Medicine's tool of choice is: Medical Capabilities assessment and status tool (M-CAST) and how this system complements the FEMA systems. M-Cast applies specific and defined capabilities against requirements of program standards providing a standard measure of readiness for a given capability. Capabilities as viewed in this system represent smallest unit teams or squads performing specific functions required for a hazard type. While being applied to specific emergency management capabilities, the program standards have broader applicability to

capabilities in general. Specifically, capabilities for response to chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) incidents should be measured against program standards and their objectives for an "all hazards" approach to emergency management.

Chapter IX is the conclusion. Reliability of communications by either military or civilian personnel is a must. The ability to share information between military and civilian entities is very important with that in mind it is my conclusion that the NJDHSS should adopt the Disaster Management Interoperability Services (DMIS). DMIS is an integral part of the President's Disaster Management e-Government Initiative focused at significantly enhancing Disaster Management on an interagency and intergovernmental basis.

DMIS is built "from the bottom up" in recognition of the fact that all disasters – no matter how consequential or large-scaled – are first encountered by local responders. DMIS tools provide the ability to describe an incident and make specific needs requests in enough detail for shared situation awareness with other organizations that may be called upon to help

THIS PAGE INTENTIONALLY LEFT BLANK

II. INCIDENT COMMAND SYSTEM

Incident Command System (ICS) is an organizational tool that can be thought of as both a requirement of public health and disaster response agencies and as an internal requirement for good emergency response management. Disaster events may involve exuberant numbers of personnel, whose activities must be carefully coordinated, and multiple agencies that must quickly establish effective ways of interfacing with each other and, in a unified fashion, with the public.

ICS is an organizational tool, employed by emergency response agencies to maximize the effectiveness of their response. Law enforcement, fire departments, and DOD have long used this system. Public health agencies have realized the necessity of identifying how to fit into the larger ICS and how to apply it internally to make their emergency response more effective. To be prepared for emergency mobilization, the MCC must establish its own internal incident command structure and activation procedures. This framework must be established prior to any event and frequently tested and evaluated.

ICS provides the following key management functions:

- Minimizes the span of control.
- Maintains unity of command.
- Keep decisions and resource allocations prioritized and objective-driven.
- Uses common terminology.
- Creates and follows an action plan.

ICS begins with establishing lines of authority and communication to be followed when an event occurs (see Figure 1, below). Roles and responsibilities are pre-assigned and are based on job title. The Command staff consists of the Incident Commander and the Liaison, Information, Safety, Operations, Planning, Logistics, and Finance and Administration Offices.

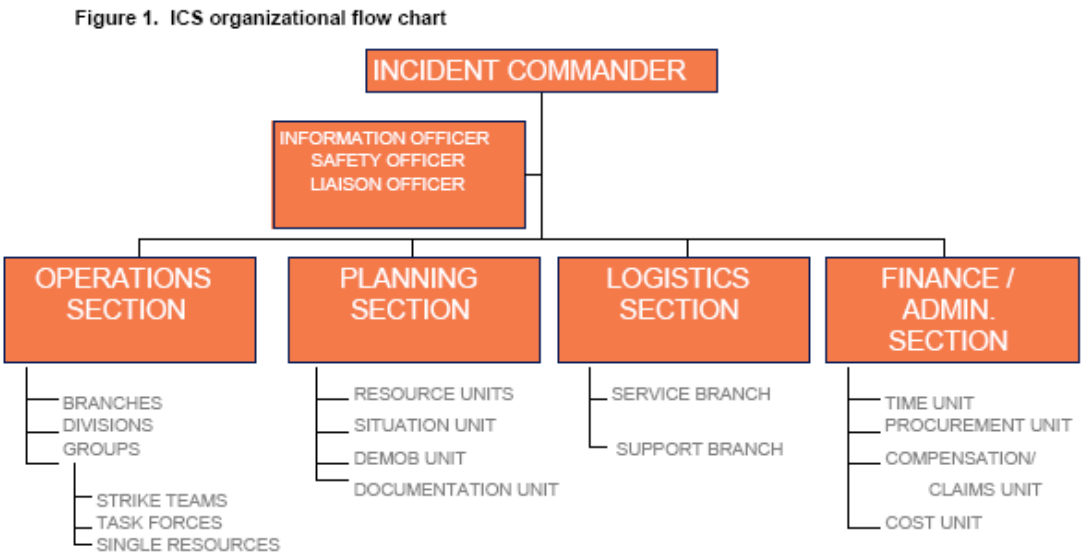


Figure 4. ICS Organizational Flow Chart (From: NRP)

The Incident Commander has the ultimate responsibility for determining event objectives and strategies. The Information Officer coordinates all information dissemination and clears all information releases. If an information point person is not made readily available to the media or is not prepared to provide accurate information that addresses the public's concerns, the media should conduct its own risk interpretation and should disseminate its own conclusions to the public. In the case of a possible bioterrorist event, information control can be a more sensitive issue if, for example, a criminal investigation is concurrent with the event management. In the case of an event involving human patients, there are additional concerns for privacy of victims and sensitivity to victims' families. The Safety Officer anticipates, detects, and corrects unsafe situations. The Liaison Officer serves as a contact point for representatives of assisting and cooperating agencies. The Operations Section develops the strategy portion of the Incident Action Plan, participates in the planning process, and accomplishes the incident objectives. The Planning Section maintains resource status, gathers and analyzes data, provides displays of situations, estimates future probabilities, and prepares alternative strategies. The Logistics section manages the allocation of personnel, equipment, services, and support. This section is responsible for management of internal communications equipment and strategies. The section also is responsible for

procurement and for servicing equipment. The Finance and Administration Section should provide financial management and accountability. They should authorize expenditures, maintain disaster records, maintain injury and damage documentation negotiate vendor contracts, and establish any formal agreements with other agencies. ICS is flexible, allowing for a systematic approach that can be expanded or collapsed as needed, depending on the level of response required for a specific incident. ICS allows for multiple emergency response agencies to effectively coordinate to maximize resource utilization and improve communication while minimizing confusion, proliferation of misinformation, and duplication of efforts.

The next chapter gives us a bird's eye view of the general organization of a Disaster Response Plan. As we have seen thus far, all Civilian Health Care activities (public or private) and Military Treatment Facilities (MTF's) are required to have a contingency plan and/or emergency plans. An Emergency plan comprises a structured collection of actions that must be followed to adequately respond to an anticipated set of scenarios. The emergency plan shall describe the resources required, including human and material resources, ancillary documentation, such as maps, simulation results, lists of authorities to contact, etc as described in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ORGANIZATION OF THE NEW JERSEY DEPARTMENT OF HEALTH AND SENIOR SERVICES PLAN (NJDHSSP)

The NJDHSSP should be a base plan that provides the region with a comprehensive approach to managing all domestic contingencies. When fully developed, the NJDHSSP should not be an umbrella for existing Regional incident management plans; rather, it should build upon or incorporate what is best in the current plans of Regional, State, and local agencies, as well as those of private voluntary organizations, non-governmental organizations, and the private sector.

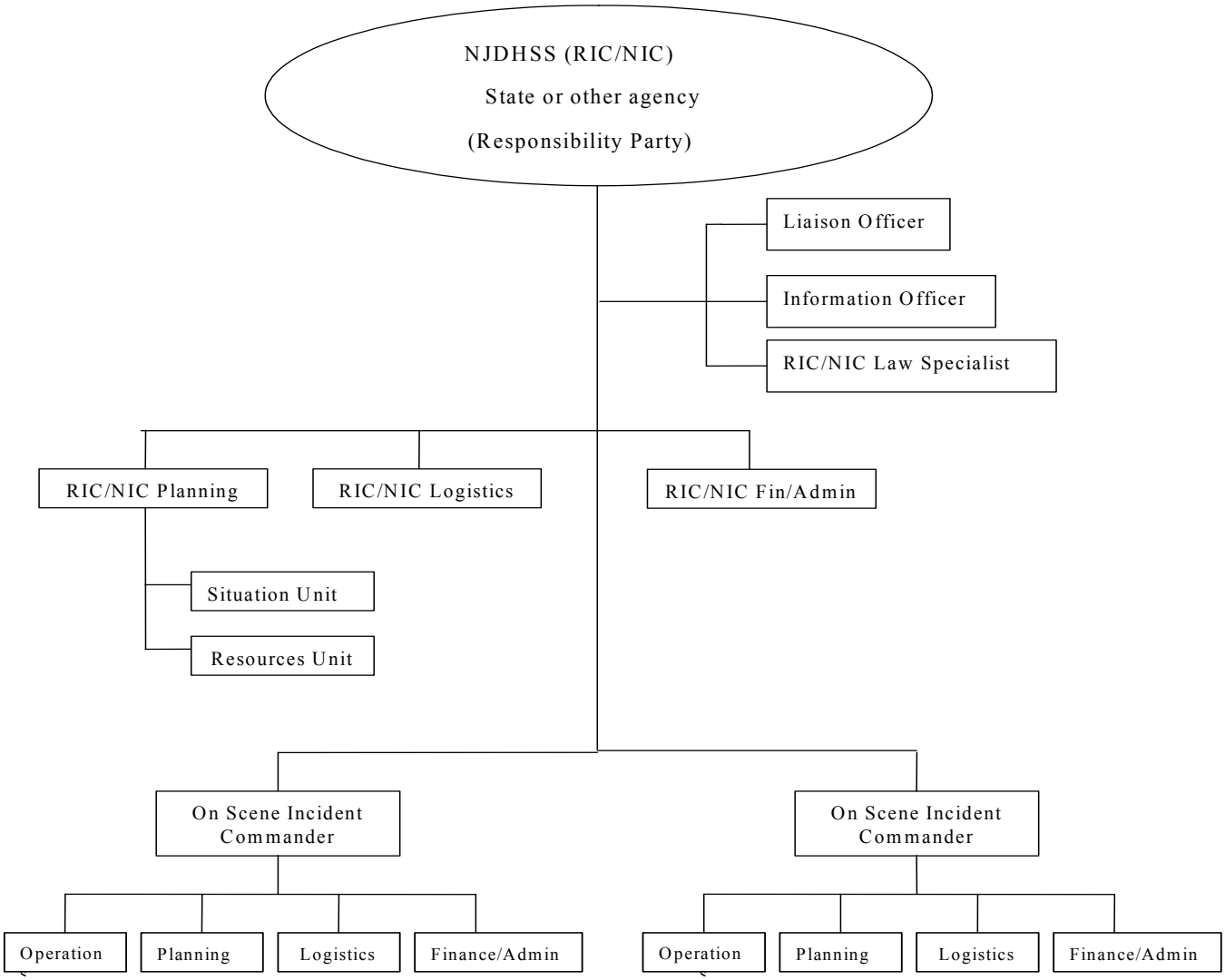


Figure 5. NJDHSS Proposed Flowchart

The primary elements of the NJDHSSP as envisioned in this initial Plan are as follows:

A. THE ROLES AND RESPONSIBILITIES

This section should describe the activities of local, State, and Regional authorities and non-governmental organizations (NGO's) and the private sector in managing domestic contingencies. A key element in the NJDHSSP is the distinction between the ongoing responsibilities of the Head and the responsibilities of the Incident Commander (IC) and Supporting Agencies (SAs) in the context of a given contingency.

In keeping with the National Strategy for Homeland Security and HSPD-5, the NJDHSS should recognize the American governmental structure with its Federal, State, and local authorities, as well as the vital roles that the private sector and the citizenry play in contributing to a robust national effort in all domains and under all contingencies. These efforts are further supported by interconnected and complementary resource coordination mechanisms and operational capabilities from all relevant entities to help ensure that essential requirements for each contingency are met.

B. STATE AND LOCAL AUTHORITIES

State and local levels of government have the primary responsibility for funding, preparing, and operating services that initially respond to an incident. For example, State and local law enforcement and health personnel provide the first line of defense in protecting critical infrastructures and public health and safety. Local police, fire, emergency medical, emergency management, public health, and other personnel are often the first to respond to an incident and the last to leave. In some instances, a Federal agency in the local area may act as a first responder to an incident, and local assets of Federal agencies may be employed to advise or assist State or local authorities with the approval of the local head of the Federal agency.

As a State's chief executive, the Governor is responsible for the public safety and welfare of the people of that State or territory. The Governor:

1. Is responsible for coordinating State and local resources to address effectively the full spectrum of actions to prepare for and to respond to man-made incidents, including terrorism, natural disasters, and other contingencies;

2. Has extraordinary powers during a contingency to suspend authority, to seize property, to direct evacuations, and to authorize emergency funds;

3. Plays a key role in communicating to the public, in requesting Federal assistance, when State capabilities have been exceeded or exhausted, and in helping people, businesses, and organizations to cope with disasters; and

4. May also encourage local mutual aid and implement authorities for the State to enter into mutual aid agreements with other States and territories to facilitate resource sharing.

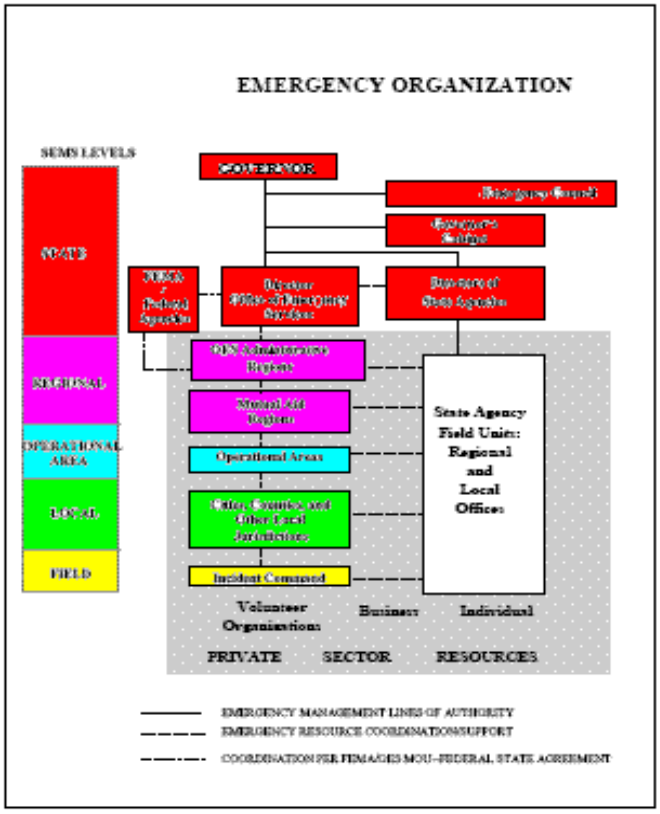


Figure 6. Emergency Organization Structure (After: NRP)

C. FEDERAL GOVERNMENT

HSPD-5 assigns specific roles and responsibilities to the Secretary of Homeland Security, other key Federal executives, and departments and agencies involved in domestic incident management. These roles and responsibilities should be exercised in conjunction with existing agency authorities and missions.

1. Secretary of Homeland Security

Under the authority of HSPD-5, the roles and responsibilities of the Secretary of Homeland Security fall in four broad areas. These are: Direction and Planning, Communications and Information, Training and Continuous Improvement, and Incident Management. As defined in Section 2 (10) and (14) of the Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135, et seq. (2002).

a. Direction and Planning

The Secretary:

(1) Directs the efforts of various Federal departments and agencies in anticipating, preventing, preparing for, responding to, or recovering from terrorist incidents, natural disasters, or other emergencies and for special events.

(2) Under relationships and mechanisms established for such purposes, directs the integration of DHS activities and various other Federal departments and agencies with those of the Attorney General, generally through the FBI, concerning domestic intelligence collection, law enforcement activities to detect, prevent, preempt, and disrupt terrorist attacks, and criminal investigations of terrorist threats or attacks.

(3) Under relationships and mechanisms established for such purposes, directs the integration of DHS activities and various other Federal departments and agencies with those of the Secretary of State when international activities are required to assist in awareness, prevention, preparation, response, or recovery activities related to a domestic incident.

(4) Under relationships and mechanisms established for such purposes, directs the integration of DHS activities and various other Federal departments and agencies those of the Secretary of Defense concerning military support to civil authorities and for Homeland Defense activities.

(5) Provides direction and assistance to State and local governments to develop all disciplines, all hazards plans and to ensure that these plans are compatible with the NRP and to ensure that adequate equipment and other capabilities are in place, that personnel are trained, and that the plans are exercised.

(6) Provides direction and assistance to the private sector to ensure that adequate planning, training, and exercise activities take place and to promote collaboration to develop sufficient capability to reduce the nation's vulnerability.

b. Communications and Information

The Secretary:

(1) Provides a core set of concepts, principles, terminology, and technologies describing the National Incident Management System.

(2) Oversees and, as appropriate, consolidates the Federal government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public.

(3) Ensures that, as appropriate, information related to domestic incidents is gathered and provided to the President; to the public, private sector, state and local authorities; and all Federal departments and agencies.

c. Training and Continuous Improvement

The Secretary:

(1) Provides standardized, qualitative reports to the Assistant to the President for Homeland Security on the readiness and preparedness of the nation to anticipate, prevent, prepare for, respond to, and recover from domestic incidents.

(2) Ensures rigorous requirements for continuous improvements through a national system to plan, equip, train, exercise, test, and evaluate and to provide standards and credentialing for homeland security.

(3) Directs and supervises specific grant programs of the Federal government for State and local governments and the private sector.

(4) Develops a comprehensive program for research and development (R&D) conducts basic, applied and advanced homeland security R&D; and facilitates the development of technical standards for homeland security.

d. Incident Management

The Secretary:

(1) Is the Principal Federal Official for domestic incident management.

(2) Provides direction for Federal operations for incident management within the United States to prepare for, respond to, or recover from terrorist attacks, major disasters, and other emergencies; and

(3) Provides direction for the application of the Federal Government's resources utilized in response to or recovery from domestic incidents if and when any of the following conditions or thresholds apply:

a. A Federal department or agency acting under its own authority requests the Secretary's assistance.

b. The resources of State and local authorities have been overwhelmed and Federal assistance has been requested.

c. More than one Federal department or agency has become substantially involved in responding to an incident, or

d. The President directs the Secretary to assume responsibility for managing the domestic incident.

The below tables are a summary of the Secretary's responsibilities during natural disasters as well as terrorist or criminal events:

NATURAL DISASTERS					
SECRETARY'S ROLES	*AWARENESS*	*PREVENTION*	*PREPAREDNESS*	*RESPONSE*	*RECOVERY*
DIRECTION AND PLANNING					
COMMUNICATIONS & INFORMATION					
TRAINING & CONTINUOUS IMPROVEMENT					
INCIDENT MANAGEMENT					
FUNCTIONAL AREA	*AWARENESS*	*PREVENTION*	*PREPAREDNESS*	*RESPONSE*	*RECOVERY*
INFORMATION / INTELLIGENCE / WARNING	DHS - IAIP	DHS - IAIP	DHS - IAIP	DHS - IAIP	DHS - IAIP
INTERNATIONAL COORD	DOS		DOS	DOS	DOS
TERRORISM PREPAREDNESS					
DOMESTIC COUNTERTERRORISM					
BORDER & TRANSPORTATION SECURITY					
INFRASTRUCTURE PROTECTION	DHS - IAIP	DHS - IAIP	DHS - IAIP		
HOMELAND DEFENSE				DOD	DOD
EMERGENCY MANAGEMENT			DHS - EPR	DHS - EPR	DHS - EPR
LAW ENFORCEMENT				DOJ	DOJ
CBRNE HAZARD	DHS - EPR		DHS - EPR	DHS - EPR	DHS - EPR

Table 1. Secretary's Role during Natural Disasters (From: NRP)

TERRORIST OR CRIMINAL INCIDENTS					
SECRETARY'S ROLES	*AWARENESS*	*PREVENTION*	*PREPAREDNESS*	*RESPONSE*	*RECOVERY*
DIRECTION AND PLANNING					
COMMUNICATIONS & INFORMATION					
TRAINING & CONTINUOUS IMPROVEMENT					
INCIDENT MANAGEMENT					
FUNCTIONAL AREA	*AWARENESS*	*PREVENTION*	*PREPAREDNESS*	*RESPONSE*	*RECOVERY*
INFORMATION / INTELLIGENCE / WARNING	DOJ-FBI	DOJ-FBI	DOJ-FBI	DOJ-FBI	DOJ-FBI
INTERNATIONAL COORD	DOS	DOS	DOS	DOS	DOS
TERRORISM PREPAREDNESS			DHS - BTS		
DOMESTIC COUNTERTERRORISM	DOJ-FBI	DOJ-FBI	DOJ-FBI	DOJ-FBI	DOJ-FBI
BORDER & TRANSPORTATION SECURITY	DHS - BTS	DHS - BTS	DHS - BTS	DHS - BTS	DHS - BTS
INFRASTRUCTURE PROTECTION	DHS - IAIP	DHS - IAIP	DHS - IAIP		
HOMELAND DEFENSE	DOD	DOD	DOD	DOD	
EMERGENCY MANAGEMENT			DHS - EPR	DHS - EPR	DHS - EPR
LAW ENFORCEMENT				DOJ	DOJ
CBRNE HAZARD	DHS - EPR	DHS - EPR	DHS - EPR	DHS - EPR	DHS - EPR

Table 2. Secretary's Role during Terrorist or Criminal Incidents (From: NRP)

D. REGIONAL AND NATIONAL INCIDENT COMMANDS

In situations where there is a need for senior executive-level response coordination, command and control of an incident may include the use of a Regional or National Incident Command (RIC/NIC). The purpose of a RIC/NIC organization is to oversee the overall management of the incident(s), focusing primarily on strategic assistance and direction and resolving competition for scarce response resources. This organization does not supplant the IC(s), but supports and provides strategic direction. Execution of tactical operations and coordination remains the responsibility of the IC(s)/UC(s).

Regional Incident Command - A RIC is an organization activated by the District Commander to ensure coordination for Command, Planning, and Logistical matters. The need for a RIC may arise when there are multiple on-scene ICs, multiple organization ICs and/or when there is heavy demand for Military resources from other agencies such as the Federal Emergency Management Agency (FEMA). The RIC will determine which critical resources are sent to which incident and determine priorities for their assignment. It is the desire of the NJDHSS to act as the RIC organization.

National Incident Command - A NIC is an organization that is functionally similar to the RlC and is used if the incident requires the direct involvement of the most senior Military Operational Commander(s).

E. PRIVATE SECTOR

1. Nongovernmental organizations, including voluntary organizations, provide essential services to victims regardless of their eligibility for Federal or State assistance. Volunteers enhance community coordination and action at both the national and local levels.

2. As the principal provider of goods and services and the owner of approximately 85 percent of the national infrastructure, private business and industry play a significant role in helping to mitigate the physical effects and economic costs of domestic incidents. Business and industry collaboration with governments and other organizations are essential for protecting and restoring the nation's critical infrastructure in the event of an incident.

a. To enhance their preparedness before an incident, businesses are urged to identify their risks, develop appropriate contingency plans, and take corrective actions to enhance their overall readiness.

b. Businesses and industry can supply critical resources, can assist in restoring essential services in the short term, and can help rebuild the economic base as part of the recovery effort.

F. CITIZENRY

As residents in their communities, citizens are active in preparing for and responding to a variety of emergencies and events. Strong partnerships with citizens and their communities are another vital support element of the national framework involving awareness, prevention, preparedness, response, and recovery.

As we move along from a Top-down view the next chapter will provide specific guidance or the organization of the Disaster Plan itself.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ORGANIZATION OF A DISASTER PLAN

This chapter will describe the principal aspects of the Domestic Incident Management System (DIMS) and makes initial assignments to Regional agencies regarding their responsibilities with respect to each of the functional areas and domains that describe the life cycle of an incident. Additionally, this section describes how domestic incidents should be managed, using procedures outlined in this Plan, in concert with the procedures and coordinating structures contained in existing Regional plans, until full implementation of the approved NJDHSSP.

The NJDHSSP should be a living document that should constantly be revised in response to new information, new situations, new technology, lessons learned and refined procedures.

A. FUNCTIONAL AREA PLANS

This section should be developed for each functional area by the Program Manager, in coordination with all of the Department Heads involved in the functional area. These plans should describe the tasks that should be performed within the functional area, identify potential assignments for each section, and define the coordination mechanisms by which functional area assessments should be conducted, and by which support to awareness, prevention, preparedness, response, and recovery activities should be coordinated.

B. DEVELOPING A DISASTER PLAN

Before an organization can begin to develop a disaster plan, there must be full commitment from all management levels and this process must be assigned a high level of priority. It is important that key program staff be involved at various levels of plan development and implementation for the plan to be successful. It must also be understood that developing an emergency response plan is an ongoing process, not a task to be

completed and filed on a shelf. To have an effective response to an emergency, NJDHSS plan must be carefully developed, appropriate to their needs, routinely reviewed and updated, and practiced.

1. Objectives

- Establish disaster planning as a high priority.
- Obtain full support, conceptually and financially, for plan development and maintenance.
- Develop a comprehensive disaster response plan.

2. Before the Incident

- Select/Identify an individual or group of individuals to develop the plan. The size of the team will depend on the level of the program's responsibilities, operations, and resources.
- Obtain approval of upper management to authorize the time needed for the planning process.
- Empower the team, in writing, with the authority and responsibility of plan development and maintenance.
- Issue a “Mission Statement” to define the purpose of the plan and the authority and structure of the planning group; include financial support.
- Establish a work schedule and planning deadlines for the planning team.
- Identify internal resources and capabilities.
- Gather information about your current responsibilities, capabilities, and response expectations.
- Identify the laws and regulations that provide the specific authority for the program to conduct its activities. Be sure to consider the New Jersey Heath and Safety Code, New Jersey Code of Regulations, and other statutes and regulations applicable to the program.
- Identify critical operations that will be given priority in an emergency.
- Develop Emergency Operations Center (EOC) organization structure and staffing list.

- Identify the reporting relationships and chain of command required to contact the NJDHS Emergency Operations Center (CDHS EOC), and applicable emergency operations centers at the local level.
- Develop a relationship with the individual(s) who represent your activities at the (NJDHS EOC) during a disaster.
- Ensure that the plan includes a response to incidents that do not rise to the level of "declared disasters" but may require increased public and environmental health response such as hazardous material incidents, food borne illness outbreaks, etc.
- Contact the local emergency planning office for communities with program field offices to determine the typical emergencies to which program staff may need to respond, i.e., earthquakes, fires, floods, and hazardous materials releases. Review and identify your program facilities that can be impacted by those events.
- Identify how program staff will respond to the event to protect public health.
- Determine if there are other vulnerable program facilities or areas that could be impacted and ensure that the emergency plan includes these hazards.
- Establish guidelines that identify various levels of plan activation and appropriate personnel to respond.
- Determine specific goals for the plan development team and set achievable objectives and timelines.
- Make a list of tasks to be performed and assign responsibilities within the team.

C. PLAN ELEMENTS

Include the following elements in the plan:

Introduction

- Provides a brief overview of the purpose for the plan

Authorities and References

- Provide lists of legal authorities that allow the program to conduct its activities

Emergency Management Organization

- Describes the emergency management structure in place for the program and how the program fits into the local, regional, or state response structure.
- Identifies who is in charge
- Describes the continuity of management for the program
- Establishes compliance with the Standardized Emergency Management System
  (SEMS)
- Provides a description of the Incident Command System and how it relates to the field response activities.

Concept of Operations

- Describes the emergency response procedures (plan activation, call down etc.) that will be implemented.
- Describes the role of each unit within your program.
- Identifies how priorities will be set.
- If applicable describes structure and organization of EOC.
- Describes how mutual aid or supplemental resources will be requested or provided and how outside resources will be integrated into the program's response.
- Description of field response and relationships to JEOC.
- Relationships with federal agencies.

Supporting Documents and Appendices

- Includes supporting documents such as detailed procedures, checklists, phone rosters, resource lists, lists of useful acronyms, a glossary of terms, etc. Also includes copies of forms necessary for financial record keeping and reporting response status.

Incorporate the plan into the program's operations including:

- Conduct orientation sessions for staff
- Ensure that all staff understands their role in an emergency.
- Conduct emergency exercises both internally and in coordination with other agencies.

- At least annually, evaluate and modify the plan as necessary.

D. DURING THE INCIDENT

- Activate the phases of the plan as appropriate.
- Review the elements of the plan and make changes as needed.

E. AFTER THE INCIDENT

- Conduct an in-depth review and critique of response activities and the emergency plan with staff and with other organizations or agencies with which they interacted. Review all activities associated with the incident and make recommendations for change.
- Create a detailed after-action report on all activities of the program during the incident.
- Make adjustments to the plan based on the lessons learned during the response.

Below is the current NJDHSS Health Command Center Organizational Structure:

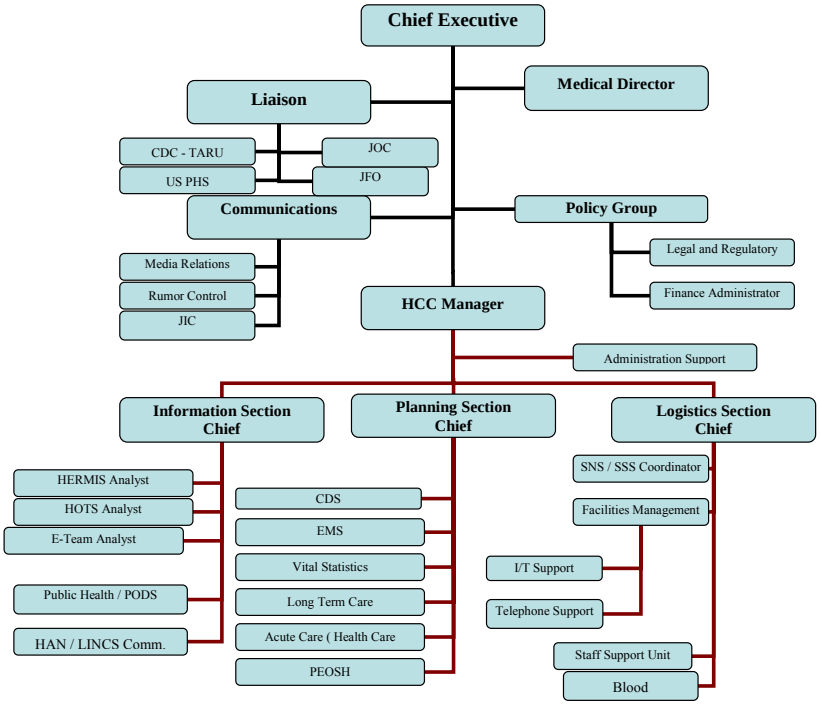


Figure 7. NJDHSS Organizational Chart (From: NJDHSS)

The DHSS has created the Medical Coordination Center (MCC) Program within the Division of Health Emergency Preparedness and Response. The MCC Program is developed and supervised by the Division of Health Emergency Preparedness and Response, MCC/DHSS Coordinator. The MCC Program will be enhanced and staffed by additional MCC regional personnel. The DHSS has created five (5) health planning regions based a statewide threat assessment and a variety of hazard vulnerability factors to include: population, population density, location of health care facilities, as well as identified high risk hazards.

The MCC Program is designed to enhance statewide coordination capability and to maintain the integrity of New Jersey's public health care system(s) in order to minimize the effects of public health, health care or mass casualty incidents (MCI).

Now that we have discussed the roles and responsibilities and how the plan should be structured, the next step is to look at specific elements that are needed to develop a comprehensive Disaster Response plan such as the assumptions, considerations and guiding principles.

V. ASSUMPTIONS AND CONSIDERATIONS

A. PLANNING ASSUMPTIONS AND CONSIDERATIONS

1. A Single Plan

The New Jersey Department of Health and Senior Services (NJDHSS) should integrate existing State domestic awareness, prevention, preparedness, response, and recovery plans in to one base plan, addressing functional areas common to most contingencies, including annexes that describe unique procedures required under special circumstances.

2. An "All Hazards/All Disciplines" Plan

Current emergency plans are designed to deal with particular types of contingencies. In keeping with the requirements of HSPD-5, I would advocate that NJDHSS prepares a single plan that is flexible enough to accommodate 'all hazards,' covering all of the disciplines required for conducting activities throughout the 'Life Cycle' of an incident. Under the NJDHSS, 'hazards' plan should refer to the full range of possible contingencies, including:

a. Natural Disasters

Such as floods, earthquakes, hurricanes, tornadoes, droughts, and epidemics;

b. Accidents

Such as chemical spills, industrial accidents, radiological or nuclear incidents, explosions, and utility outages;

c. Civil or Political

Incidents including mass migrations, the domestic effects of war, nation-state attacks, and unrest or disorder resulting from riots, public demonstrations, and strikes.

d. Terrorist or Criminal

Incidents including chemical, biological, radiological, nuclear, explosive, or cyber threats or attacks; and

e. Significant Events and Designated Special Events

Requiring security, such as inaugurals, State of the Union addresses, the Olympics, and international summit conferences. These contingencies are not mutually exclusive and may occur individually, simultaneously, or in combination.

3. A Plan that Emphasizes Unity of Effort among All Levels of the Region

The NJDHSS plan should emphasize unity of effort among all levels of the Region. Under this Plan, Federal, State, and local governments, including private organizations and the American public, should work as partners to manage domestic contingencies efficiently and effectively. There is pressure from Federal, State and local agencies as well as industry associations, including the Department of Homeland Security and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) for a better regional response planning. In addition JCAHO has made emergency preparedness one of its seven public policy initiatives and has increased its accreditation requirements in that area. Healthcare providers have begun to take into account the need for more regional planning since disasters can cross city and state boundaries.

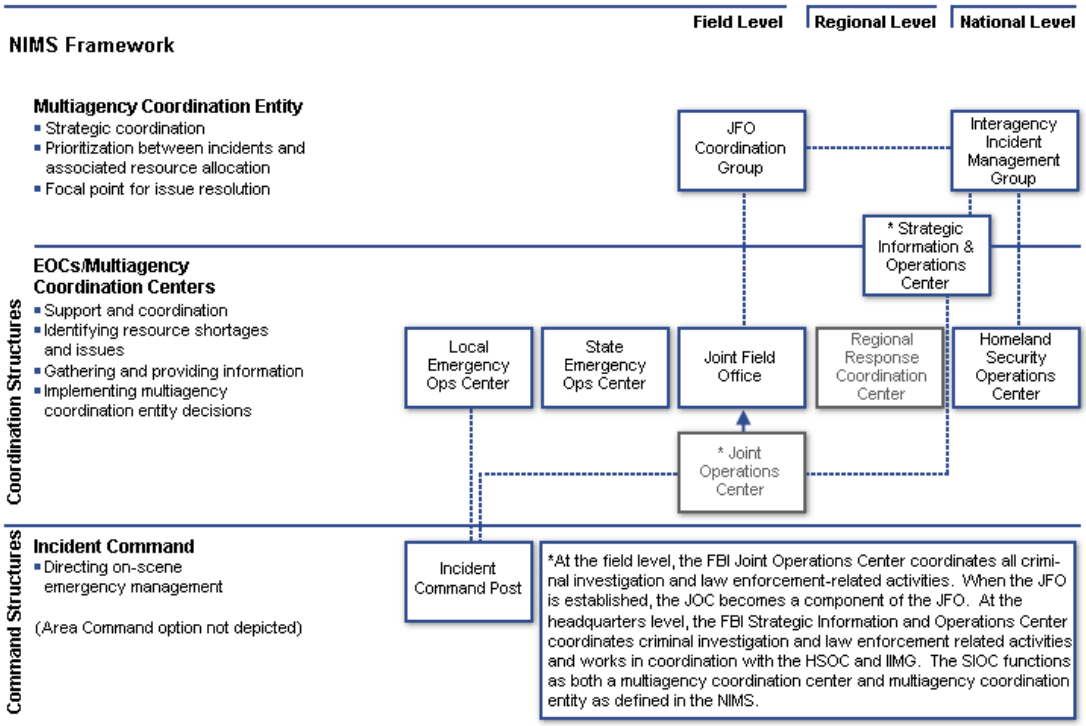


Figure 8. Incident Command Post (From: NRP)

4. A Plan that Integrates Crisis and Consequence Management

In keeping with the Presidential Directive, the NJDHSS should "treat crisis management and consequence management as a single, integrated function, rather than as two separate functions."

5. A Plan that Places the Same Emphasis on Awareness, Prevention, and Preparedness, Traditionally Has Been Placed on Response and Recovery

Traditionally, response plans have been exactly what their name implies—plans for responding to and recovering from an incident or contingency. In the aftermath of September 11, 2001, however, preventing terrorism and reducing our nation's vulnerabilities through preparedness have become top priorities. The NRP (National Response Plan) set forth a new concept of a 'response' plan by covering five domains: Awareness, Prevention, Preparedness, Response and Recovery which NJDHSS should follow.

B. GUIDING PRINCIPLES

In addition to the imperatives set forth in HSPD-5, the following fundamental principles guide the development of the NJDHSS:

1. Fundamental Role of State and Local Authorities

The NRP recognizes that domestic contingencies generally begin and are initially responded to as local events. The vast majority of events are dealt with at the State or local level. Federal involvement should not be necessary in many instances, except for reporting.

2. Importance of Effective Communication

Information sharing between agencies is critical for the ultimate success of a regional plan. The NJDHSS requires effective information sharing among all affected parties. Timely reporting is vital for informed decision making at all levels.

3. Primacy of Preserving Human Life

Preserving human life constitutes the first priority under the NJDHSS, during the execution of activities under this Plan. Preserving human life should always take precedence over all other responses and recovery requirements.

4. Seamless Transitions

The NJDHSS plan should include mechanisms to provide seamless transitions that must occur on several levels. To be effective, operations must transition smoothly from simple to complex situations and from routine, day-to-day operations to catastrophic incidents.

5. Standardization of Systems, Procedures, and Communications

Effective incident-management operations require interoperability and compatibility in systems, procedures, and communications. Through the Medical Coordination Center System (MCCS), this Plan should provide a core set of concepts, principles, terminologies, and technologies. Agencies and authorities are expected to conform to the standards of the NJDHSS and the MCC.

6. Integration of Best Practices

To capitalize on what has been deemed effective in the past, the NJDHSSP should incorporate best practices from previous plans and agencies, as well as exercises and actual experience. Additionally; the NJDHSSP and the MCC should contain required processes to ensure continuous improvement and vulnerability reduction through lessons learned and other feedback. The MCCS should also include processes for taking advantage of research and development and technological advances.

7. Need for an Agile Incident Management Capability

To support this requirement, the NJDHSSP must be:

a. Scalable

The NJDHSSP can be utilized to cover the spectrum from day-to-day incident management activities to the most complex and severe contingencies, including catastrophic events.

b. Modular

The NJDHSSP should be designed so that some or all of its components can be tailored to fit the specific requirements of a situation.

c. Flexible

The NJDHSSP should be able to address new threats and risks. It should also address the need to implement changes to operational procedures based on lessons learned such as the TOPOFF 3 exercise and other feedback mechanisms.

8. Ability to Accommodate State and Local Systems

When implemented, the NJDHSSP and the MCCS should be flexible enough to accommodate State and local incident management systems.

The below figure represents how the different plans relate to each other:

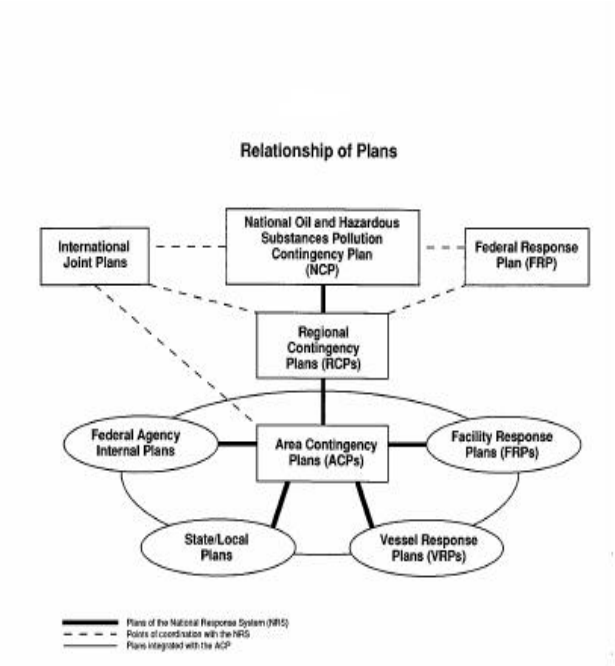


Figure 9. Relationship of Plans (From: NIMS)

There is a great quote "People are the most forgotten part of the organization" by Dr. Ambuj Goya, General Manager of Lotus Software. According to Ambuj, the untapped resources in organization are human responsiveness, awareness, and ingenuity. In today's environment it's necessary to integrate the people which bring me to my next chapter which is the Life Cycle of incident activities. The life cycle is best described as containing five domains within which domestic incident management activities occur: awareness, prevention, preparedness, response, and recovery.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. THE "LIFE CYCLE" OF INCIDENT MANAGEMENT ACTIVITIES

HSPD-5 calls for a plan that addresses the entire universe of incident management from pre-incident awareness, prevention, and preparedness to post-incident response and recovery. As previously mentioned, the NJDHSSP should follow this directive as well.

A. DESCRIPTIONS OF THE LIFE-CYCLE DOMAINS

The life cycle of activities is best described as containing five domains within which domestic incident management activities occur: awareness, prevention, preparedness, response, and recovery. A key element of the domain life cycle concept is the recognition of the critical importance and need for continuous improvement, via feedback mechanisms, lessons learned, evaluations, research and development, the adoption of best practices, and other dynamic processes.

1. Awareness

According to the National Response plan "Awareness refers to the continual process of collecting, analyzing, and disseminating intelligence, information, and knowledge to allow organizations and individuals to anticipate requirements and to react effectively". It involves an interactive process of sharing, evaluating information from multiple sources to include the fusion of domestic and international intelligence and operational reports into a coherent picture. It also includes communications and reporting activities and activities to forecast or predict incidents and to detect and monitor threats and hazards. It also covers public education. Awareness activities are the bases for advice, alert and warning, intelligence and information-sharing, technical assistance, consultations, notifications, and informed decision-making at all interagency and intergovernmental levels, as well as with the private sector and the public.

2. Prevention

Prevention refers to actions to avoid an incident, to intervene to stop an incident from occurring, or to mitigate an incident's effects. It involves actions to protect lives and property, and defend against attacks. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence

operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health surveillance and testing processes; immunizations, isolation, or quarantine; and law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity.

3. Preparedness

Preparedness refers to the activities necessary to build and sustain performance across all other domains. In one sense, preparedness is part of the life cycle of a specific incident in that it includes a range of deliberate, time-sensitive tasks that need to occur in the transition from prevention to response. Preparedness can also be characterized as a continuous process or cycle. The mission of preparedness is to develop meaningful answers to the question, "Are we prepared to be aware of, to prevent, to respond to, and to recover from terrorist attacks, major disasters, and other emergencies?" Preparedness involves efforts at all levels of government and within the private sector to identify risks or threats, to determine vulnerabilities, to inventory resources available to address those vulnerabilities, identify requirements or shortfalls, resulting in a preparedness plan to remedy shortfalls over time. Preparedness plans include program initiatives for planning, training, equipping, exercising, and evaluating capability to ensure sustainable performance in order to prevent, prepare for and respond to incidents.

4. Response

Response refers to the activities necessary to address the immediate and short-term effects of an incident, which focus primarily on the actions necessary to save lives, to protect property, and to meet basic human needs. Life-saving and life-protecting activities take precedence over other critical actions. Response activities include assessing preliminary damage and unmet needs; activating and deploying response resources into an affected area; providing access to and mobility within the area of operations; developing, coordinating, and executing an integrated incident management plan (which includes the activities of all response agencies); allocating existing resources in support of the plan and obtaining additional resources as required; and deactivation and standing down. It includes activities for providing basic life-support functions and services, triaging and treating personal injuries, minimizing damage to the environment

and to property, both public and private, and planning for the transition from response to recovery within each functional area. Response operations also include law enforcement, investigative, and security activities conducted to address the criminal aspects of the incident.

5. Recovery

Recovery refers to those actions necessary to restore the community back to normal and to bring the perpetrators of an intentional incident to justice. It entails the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons: additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents. It may also include prosecution, incarceration, or other forms of punishment against perpetrators of intentional acts, as well as the seizure and forfeiture of their property (lessons learned from Katrina).

Domain activities are neither linear nor mutually exclusive. There is no temporal or functional dividing line between or among domains. For example, there are broad and sustained awareness, prevention, and preparedness activities. There are also specific awareness, prevention, and preparation activities for a particular incident that can be undertaken while response or recovery activities are under way. Recovery operations may start simultaneously with response operations. Lessons learned in the conduct of activities in any of the domains should likely inform the enhancement or initiation of activities in several domains.

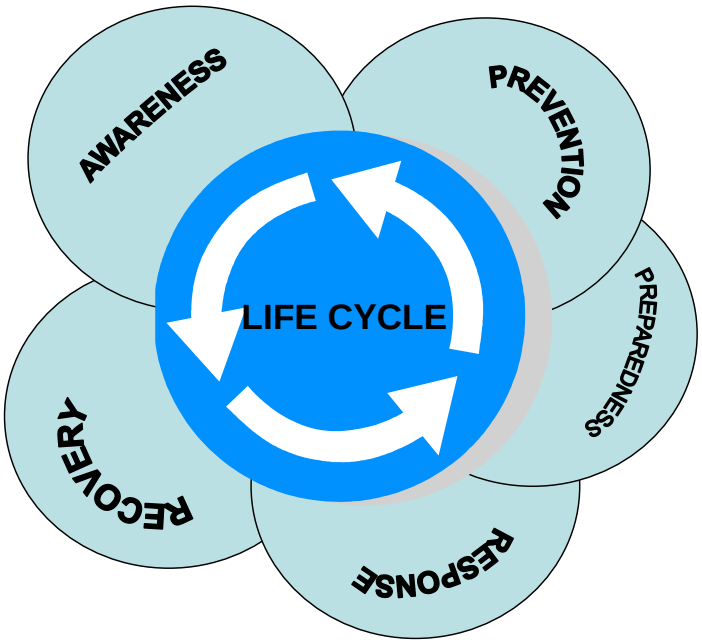


Figure 10. Life Cycle of Incident Management Activities

B. REGIONAL MECHANISMS TO SUPPORT LIFE-CYCLE OPERATIONS

Examples of mechanisms for awareness, prevention, and preparedness, include:

1. Threat, risk, and vulnerability assessments
2. Information management and intelligence coordination
3. Grant assistance
4. National training and exercise system

The NJDHSSP should also outline mechanisms for incident management, which can be detailed in the MCCP. For example, the Head may (either before, during, or after an incident) designate Regional incident management officials to serve as the NJDHSS representative to oversee Regional incident management activities in the field at the regional, State, or local level. In certain circumstances, the Head may designate a high-ranking Regional official to serve as the Regional senior representative in the field for the purpose of overseeing all Regional incident management activities (see figure 1).

C. ENSURING PRIVACY OF MEDICAL INFORMATION

The communications model incorporates technology channels (e-mail, Internet, facsimile) could potentially place personal health information at risk. Health-Care organizations are required to adhere to Privacy Act standards, and the model must comply with these standards. U.S. Law requires security of health and personal data. The model must meet these established requirements. Confidentiality is a tool for safeguarding privacy. Health-care organizations are required by law to follow privacy and data security standards. The communications model must also comply with these standards. Privacy of personal medical information is ensured under the following U.S. laws:

- Privacy Act of 1974
- Copyright Act of 1976
- Medical Records Confidentiality Act of 1995
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Children's Online Privacy Protection Act of 1999

1. Ensuring Data Integrity

We assure the accuracy and completeness of data by archiving and retrieval processes, establishment of redundant systems, and development of a disaster recovery plan. Once entered, data are unalterable. Archiving and retrieval processes are constructed so as to not allow alteration or deletion data.

2. Security of Data Files

Computerized records allow health care information to be accessed, copied, or transferred to unauthorized parties; medical information is most vulnerable when transported via the Internet. Protection of data requires methods allowing only authorized personnel access. Security involves controlling access to information, protecting it from disclosure to unauthorized persons, alteration, destruction, or loss. A security structure must be developed using:

- Encryption
- Authentication
- Firewalls
- Electronic signatures

3. Professional Licensure

By using various technology channels, the communications model has the potential to provide services across State lines. For future implementation of Level 2 service outside New Jersey, which can include medical triage, it should be necessary to define the licensure issues addressing specific State mandates or Federal models and to work with appropriate organizations to identify possible solutions.

NJDHSS participated in a TOPOFF-3 exercise (April 2005), during this exercise communications as they relate to chain (wiring diagram), networking, and substance received the most comment. Chain of communication was important, although vertical systems are usually very effective, lateral and diagonal networking was either not evident or efficient. For example, when an issue or event took place, those in the vertical chain were made aware, but parallel agencies were not, in all cases, kept informed. The result is a lack of information that could have a decided impact on the ability of other agencies to respond as needed. The inability to share information in a direct fashion, affects coordinated response and reduces the ability to place resources and support where they would be most needed (TOPOFF-3 after action report).

The next chapter provides information about the current state of NJ communications and available technologies. This chapter is necessary to address the communications network program and system redundancy. During the exercise, the routine method of conveying information was through email--familiar and routine. It is recommended that a review of networking protocols be completed at the state and local level so that internal, external, and cross-agency information can be shared as quickly as possible. An examination of some of the county communications systems, to include recommended similar systems at the municipal level and state level, may be in order.

VII. AVAILABLE TECHNOLOGIES

There are several available technologies. As part of my thesis, I was able to attend the 2006 National Disaster Management Systems (NDMS) conference, held in Reno Nevada. During this conference I was witnessed that different systems are available to any State, or Region. It is unfortunate that we are still looking at different solutions vice settling one solution or at least a solution that would be compatible with other programs. During the conference courses no one was able to identify a single product or system to use. Even more surprising to me was that NDMS (during the entire conference courses) was never able to provide its audience with the lessons learned from previous disasters such as hurricanes Katrina and Rita. They did mentioned all the disaster that occurred during the previous year, to include 9/11, but no one was able to identify the lessons learned, what have we learned from all these disasters that we can use in the future, or any downfalls or successes. As for the National representatives, I was quite disappointed to see that even the leadership is not prepared; those who are the first responders are not prepared for what may come next.

Throughout my research I identified various suitable technologies but only one technology 'stood out above the crowd'; is the Disaster Management Interoperability Services (DMIS). DMIS is not only compatible with other systems but it was also one of the systems identified by the U.S. government as 'the system of choice.'

A. WHAT IS DMIS

Figure 11. (From: DMIS web site)

The Disaster Management Interoperability Services (DMI-Services) is an integral part of the President's Disaster Management e-Government Initiative – a larger initiative focused at significantly enhancing Disaster Management on an interagency and intergovernmental basis. DMI-Services is primarily focused on assisting individuals and organizations with crisis and consequence management responsibilities for the results of weapons of mass destruction and disasters and mitigation of all hazards. The primary mission of DMI-Services is to provide Interoperability services. DMI-Services is a service, not an application. It provides a portal for rapid and secure exchange of information between emergency management organizations, DMI-Services connectivity and functionality is also applicable to prevention, preparedness, response, and recovery at the local, state, and federal levels.

Those organizations that choose to use the DMI tool can benefit from preventing and responding to disasters. DMI-Services' connectivity is provided through a connection to the Internet, whether by phone line or wireless. Access to information is controlled by authentication and registration process. I was able to utilize this tool for several months after registering as a COG user. Data transfer is secured by the use of a virtual private network (VPN). DMI-Services functionality is constantly being reviewed and expanded to provide the best possible service to the Emergency Management community.

When I initially began using the tool, it was in version 2.0 and has since been upgraded to version 2.2, which offers several new features and updates to enrich the ability of COG (Collaborative Operators Group) Operators. In order to be in compliance with the Common Alerting Protocol (CAP), DMIS Alerts have been completely revised. These new CAP Alerts enable a COG Operator to send a message once and have it distributed over multiple networks using multiple formats - saving time, effort, and money. The new version allows operators to create a copy of an incident record for future use in similar situations. Operators can use this Save a Copy functionality for incidents such as floods, tornadoes, large fires, traffic-related incidents, etc.

B. WHAT ARE COGS

1. DMI-Services Collaborative Operational Group (COG)

COGS are a select group of operators who need to coordinate actions, communicate, and exchange disaster management information in a collaborative environment. A COG can consist of any number of Operators from multiple organizations who need to work together to respond to an incident. Examples of organizations that may form a COG include:

- An entire state or county Emergency Management (EM) Office
- Federal agencies
- Divisions of an EM Organization
- A public or private consulting organization that participates in Consequence Management
- Any combination of the organizations mentioned above

Local Fire Departments

Police Departments

Military Units

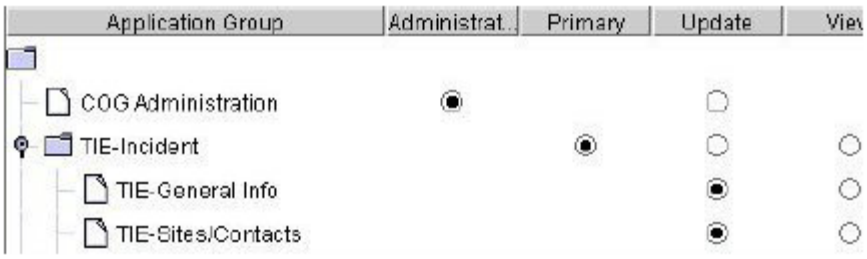
Figure 12. COG Example (From: web site)

DMI-Services functionality, exercised through COGs, supports and supplements existing emergency management organizations, relationships, policies, and procedures.

C. HOW DO COGS WORK

DMI-Services (DMIS) is a configurable set of tools that allows information to be shared throughout the professional emergency management community. In order to

improve communication and coordination during disasters, local DMI-Services Administrators and Operators need to understand how DMIS works and become familiar with its options through regular use. The ability of a COG Administrator to assign Operator roles and permissions, coupled with the ability to establish multiple COG organizations, enables organizations involved in emergency management to collaborate and exchange data at a given level and in an environment that suits their particular needs.



The roles that can be assigned are as follows:

- Administrator
- Primary Operator
- Update Operator
- View Operator
- Null Operator

Figure 13. COG Administrative View

When deciding how to organize one or more COGs, officials must determine what levels of collaboration they require on a regular basis, and consider how operating procedures may change in response to a larger-scaled incident. Potential variations of an organization's approach to establishing their COG are as numerous and complex as the organizations that play a role in consequence management. DMI-Services' flexibility in assigning roles and privileges should support many possible configurations.

D. DOES IT MATTER WHO IS A MEMBER OF A COG

Yes, it matters who is a member of a COG. Being a member of the same COG enables easier and more complete collaboration based on assigned DMI-Services roles and permissions. Operators of the same COG can see data as it is being refreshed through the **Save** command. To share information with a member of another COG, an operator must post the information to that COG. Also, the COG that receives the posted

information cannot change or edit posted information. However, they can read it, respond to it, and export data from it for import into their own applications. For example, let's say the EOC Manager and another member of the same COG are collaborating on a map. The two operators can see each other's changes when the **Save** command is selected. In order to share the map with an operator in another COG, the operator must post a copy of the Incident containing the map to that COG (assuming the operator has post permission).

The operator of the 'receiving' COG can edit a separate layer of the map (the layer belonging to his/her COG) and the operator in the originating COG should be able to view the markings in the working version of the incident. While an Operator cannot make changes to the layer belonging to another COG(s), he can use the markup as a guide to make changes to the layer(s) on the map.

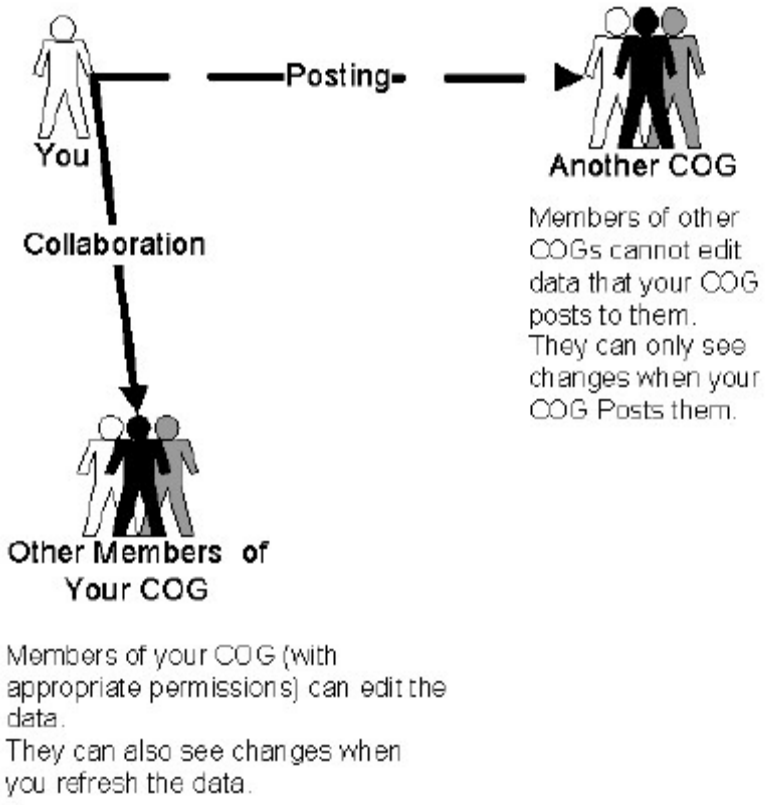


Figure 14. COG Members (From DMIS web site)

E. THINGS TO KEEP IN MIND WHEN SETTING UP A COG

When setting up a COG, we must keep in mind which operators need to collaborate and how often. COGs can use DMI-Services to communicate in two ways: internal collaboration and external sharing.

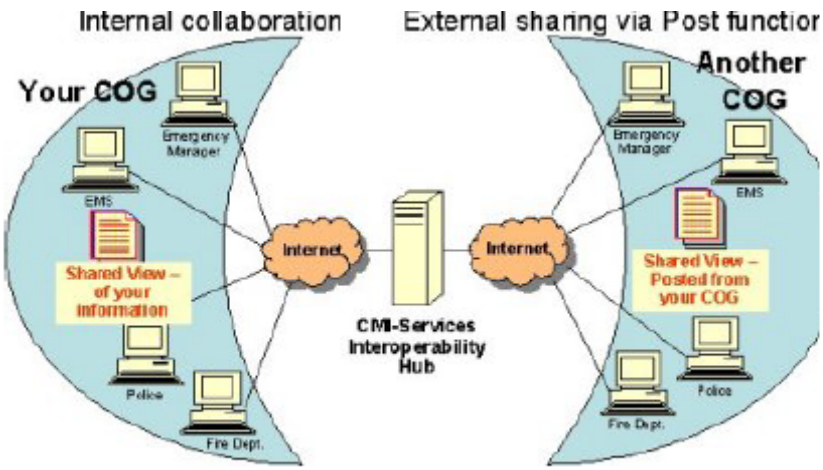


Figure 15. Internal Collaboration (From: DMIS Program)

1. Internal Collaboration

COG members can collaborate internally with their working group. That is, COG members with appropriate permissions work in a shared environment where changes are seen by everyone with the appropriate permissions in the COG as the data is refreshed (which is when an Operator saves their changes).

2. External Sharing

When COGs have a need to communicate externally, they can "post" information. Only the COGs that they select during the post process can view the information. COGs that receive posted information cannot change or edit posted information. However, they can read it, respond to it, and export data from it for import into their own applications. When starting a COG, it may be helpful to train a small "core" of users to assist the Administrator. Install DMI-Services at a few selected locations and conduct small table-top exercises using current processes and one (1) central DMI-Services Operator. As time goes on, add Operator privileges as comfort levels allow.

F. IMAGE TREND INC.

The Image Trend Resource Bridge is a web based application allowing for constant access to emergency related logistics. The Resource Bridge is used for hospital bed and resource allocation, pharmaceutical tracking, and monitoring diversion status in situations ranging from multiple-vehicle accidents to mass casualty alerts to daily operations. Special resource requests range from specific medial supply inventory to specialized doctors to bed availability. The basis of this resource allocation system is a database driven application which records all statistics relating to hospital beds and resources by category, type and status along with hospital demographics. The monitoring of this system allows for comprehensive reporting, allocation, and sharing of available beds, supplies, personnel and other resources within regions of any size from city, county, state or federal levels.

Individual views provide hospital summaries, geographical information, and more. Real-time search capabilities provide immediate status information and assignment possibilities. Through an alert notification capability users are made immediately aware of potential allocation requirements and can assess the immediate availability.

The intuitive Web-based interface of this system provides easy accessibility for various users: varying from government agencies to hospital administrators. Rights and permissions are assigned to maintain the integrity of the system. A further advantage realized through this system is straightforward content accessibility of all related information in the knowledgebase. This can involve such things as Emergency Preparedness Procedures and other references.

1. Statewide Management Console

The Resource Bridge Statewide Management Console enables administration and an aggregate view of all participating facilities. The basis of this resource allocation system is a database driven application that records all statistics relating to beds by category, type and status along with hospital demographics. The monitoring of this system allows for comprehensive reporting, allocation and sharing of available beds within a region of any size from city, county, state, or federal levels.

2. Facility Management Dashboard

The Facility Management Dashboard is the primary input tool that enables facilities to provide data on available resources. Individual views provide hospital summaries, geographical information, and more. Real-time search capabilities provide immediate status information and assignment possibilities. Through an alert notification capability users are made immediately aware of potential allocation requirements and can assess the immediate availability.

G. TVI CORPORATION

TVI Corporation is the leading manufacturer of rapidly deployable, chemical/Biological/Hazmat decontamination systems for military, public health, and first response agencies. All integrated shelter systems employ TVI's articulating frame which is covered by one or more patents. They also offer a wide assortment of accessories to support the users of our shelter systems, such as trailers, air heaters, water heaters, and air filter systems for chemical and biological filtration. TVI has supplied shelters and related concepts utilizing their own patented, specialized fabric processing technology to first responders and the military for over two decades. In addition, TVI is the leading supplier of thermal targets for military training and testing, and has also produced self-contained trailer systems utilized in the rapid deployment, emergency response scenario.

Figure 16. TVI Decon System (From TVI brochure)

Figure 17. Bethesda Naval Hospital Exercise

H. INTELLIGENT PERSONAL ASSISTANT

During my XML class we worked on a project that was based in the use of XML. The project envisioned all emergency service personnel to be equipped with specialized PDA's or cell phones which should act as intelligent personal assistants. Towards this, they propose to adopt and adapt their iPA (Intelligent Personal Assistant) framework. iPA was developed to aid its user in a ubiquitous computing environment. They designed it to run on a mobile platform (PDA or cell phone) in order to stay with its user at all times, even when she/he is mobile. Over time, an iPA "learns" about its user, building a profile to improve its own behavior with the goal of becoming a better personal assistant. It can gather, sort, and present information tailored to its user's current activities. To help protect its user's privacy, it never shares this profile with anyone.

An iPA does not require its user to ask for anything. Instead, it "learns" from what it observes from its user's actions and from anything it was "told" explicitly. Using this information, it should let its user know when something important or relevant is found, even when not asked. In this way, it becomes knowledgeable about everything going on and knows what its user wants to hear about at the right time and place.

In addition to the profile, an iPA also tailors its information gathering and delivery based on its user's current context. Context information includes current day and time, the user's location and possibly the current task being performed by the user. Location can be determined via GPS or similar positioning system if available, or from queries to nearby sensor networks. Additionally, context can incorporate other conditions supplied by the user, the current environment, or even different users and their activities and statistics.

An iPA gathers information from a variety of sources. These can include servers, both query-response and broadcast and other iPA peers. Servers could include standard database and web servers, as well as sensor networks.

Broadcast servers would ideally consist of two main channels. The first channel is a push-based channel that continuously broadcasts a data stream of XML documents. The other channel is a pull-based channel where the user or iPA can submit queries to the server requesting more detailed information about an item in the broadcast.

In the proposed scheme, it is the iPAs that should receive broadcast workflows from various crisis centers. Based on its profile, context, and user's current activities, the iPA should filter these requests and only present those that its user could participate in.

The iPA must know its user' abilities and preferences in order to be able to match requests accordingly. Originally, the iPA was targeted towards a commerce environment. This involved monitoring the habits and preferences of the user regarding restaurant choices and product purchases, tailored to different contexts. Any XML advertisement received was only given to the user depending on how well it matched these preferences, given the current user context. In a crisis management environment, the iPA instead needs to identify the capabilities and skills of the user. One way to do this is to keep statistics on the experience of the user by monitoring the incidents the user participates

in. In this way, when an XML workflow is received, its skill requirements can be matched to the expertise of the user, again taking into account the current context.

1. System Architecture

The Figure below shows a high-level view of the proposed communication architecture. Police, fire department and other services' headquarter (HQ) buildings are connected with each other and with government authorities, e.g. the state governor, by terrestrial and/or satellite networks. Likewise, when disaster site command posts are established, they are connected by terrestrial wireless or satellite links to the respective HQ. For "hot spot" on-site communications, a wireless LAN (infrastructure, ad hoc, or both) is set up. Firefighters and other personnel may be equipped with personal or body area networks, providing connectivity for sensors and terminal displays. The information flow of applications can be both horizontal, i.e. between peer entities, and vertical, i.e. along an organization's hierarchy and beyond; both push and pull information propagation are to be supported.

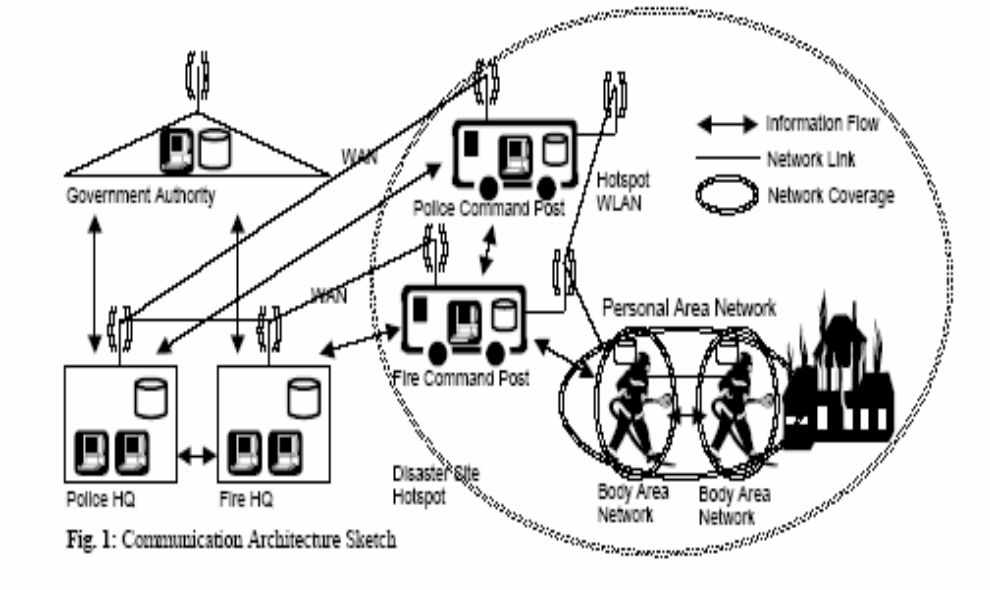


Figure 18. Communication Architecture Sketch (From: EIC)

During a crisis communication can be difficult, as communication may be unreliable, and the personnel may be scattered over different locations (and areas) and engaged in different activities. Many would be detained or unavailable entirely. Instead

of locating and contacting individuals directly, the project envisions an environment where the agency can broadcast electronically its plan of action. This broadcast should be received by both the appropriate centers as well as any available personnel through their mobile devices (e.g., PDA's), and those able to contribute to the execution of the plan can respond electronically. In the figure above for example, the fire station can broadcast a requirement for a number of police officers to go to a building to aid in its evacuation. Any officers that receive the broadcast and are able to go can reply to the call. The agency chooses those most suited from all responders, and confirms their participation. In this way, teams of emergency personnel are dynamically formed based on the requirements of executing different plans of action for the emergency situation at hand.

During the actual execution of these plans, it may become necessary to modify them. This can be due to many reasons, such as environmental changes (e.g., a building collapses or fire erupts); team members being drawn off for more critical tasks, unforeseen obstacles or delays, and so on. In order to handle such a change, all team members must be alerted, along with any monitoring centers. Using an electronic broadcast to communicate with emergency personnel provides many advantages, with improved security being one of them. With “smart” PDA’s, secure data communication becomes very inexpensive (since it is software-based), compared to the purchasing of specialized “secure” voice communication devices (e.g., military-grade walkie-talkies), which are very expensive. In this way, sensitive information and details about the emergency at hand can be transmitted to all those that could help. In addition to the improved security, using PDA’s allows for the emergency broadcast to reach a much greater pool of people, which could include for example off-duty personnel or doctors who may not be monitoring a radio or carrying around a bulky walkie-talkie, but can conveniently keep a small PDA that also has other uses. This allows such people to become “first responders”, if they are located closer to the site of the emergency, and thus drastically improve the quality of the emergency response.

2. Coordination, Monitoring, and Execution

Coordination and monitoring during the crisis involves the interaction of many different systems and individuals. Crisis centers must manage their overall workflows. This involves monitoring the progress of execution, receiving notifications from the

personnel involved, and forwarding revisions as necessary. The centers can coordinate with the individuals receive updated instructions, revised workflows, and queries. IPAs notify their users only as necessary, so as not to be too distracting. They can report to the center the current status and context of their users, and notify them of any failures or constraint violations. In some cases they can even anticipate violations or failures given current conditions and known properties. They should also report successful completions of tasks.

In the event an iPA or its user determines changes to the current workflow are necessary, the iPA can help by providing alternatives that still satisfy all requirements. If the iPA's user has sufficient authority, he/she can select one of these alternatives. The iPA should automatically notify the center and any other personnel involved. Otherwise; alternatives should be forwarded to the center for selection or approval.

In addition to helping with coordination, iPAs provide other valuable assistance during workflow execution. They provide an interface to information sources and fellow emergency personnel. Queries to various sensor networks can be initiated through an iPA. This can help with tasks such as locating victims, avoiding obstructions, and detecting dangerous environmental conditions. Since iPAs are highly personalized, information is tailored to the current specific needs of the user.

The greatest advantages of using an iPA for such applications are its own "initiative" and context awareness. Appropriate assistance can be initiated by the iPA itself, as it constantly monitors data streams for relevant information, thus freeing its user to work more effectively. Knowledge of what to monitor can be based on properties of the workflow being executed, or on observed information (e.g., from queries made by the user in the past).

I. EMERGENCY TELECOMMUNICATIONS SERVICE

Another tool that NJDHSS should considers is the used of the Government Emergency Telecommunications Service (GETS) that provides Federal, State and local government National Security and Emergency Preparedness (NS/EP) users with a ubiquitous switched voice and voice-band data communications service. GETS is used

during periods of natural or man-made disasters or emergencies that cause congestion or network outages. GETS is an emergency telecommunications service and is designed to be used when NS/EP personnel are unable to complete emergency calls through their regular telecommunications means.

The backbone for GETS is the Public Switched Network (PSN) because of its survivability, ease of use, availability, robustness, reliability, and technological currency. GETS can be accessed through the Federal Telecommunications Service (FTS), the Diplomatic Telecommunications Service (DTS) and Defense Information System Network (DISN) and is maintained in a constant state of readiness which maximizes the use of all available telephone resources in the event of congestion or outages caused by emergency, crisis, or war. Highlights of GETS Features**:**

Access Authorization: GETS access control is accomplished through the use of Personal Identification Numbers (PINs) to ensure only authorized users gain access to GETS features and protect against fraud.

Enhanced Routing: GETS calls use extensive enhancements to the PSN's robust network of interconnecting paths between switches. With these enhancements to the grid of multiple switch connections, numerous switch failures in the PSN could occur without any disruptions of GETS calls**.**

Priority Treatment: High Probability of Completion Identifier that is carried across the signaling network and used to trigger priority features such as trunk queuing and trunk reservation. Exemption from restrictive network management controls used to reduce network congestion.

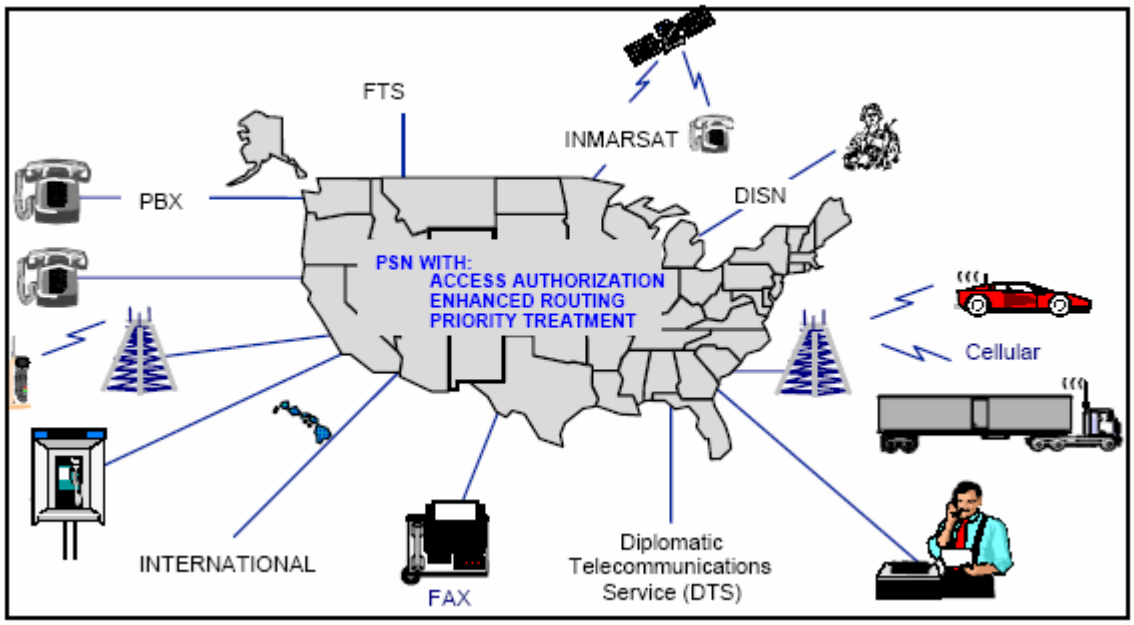


Figure 19. GETS System (From GETS Brochure)

If there is a network outages in the Public Switched Telephone Network (PSTN) then a Wireless Priority Service (WPS) would be used, the goal of a WPS is to provide an end-to-end nationwide wireless priority communications capability to **key** national security and emergency preparedness (NS/EP). Eligible users are key Federal, state, local, and tribal government and critical industry personnel who have NS/EP missions. WPS is complementary to, and most effective when used in conjunction with, the Government Emergency Telecommunications Service (GETS) to ensure a high probability of call completions in both the wire line and wireless portions of the PSTN. WPS serves NS/EP needs while minimizing impact on consumer access to the public wireless infrastructure.

Increased cellular phone usage by the general public in emergency situations regularly results in extreme network congestion, preventing key national security and emergency response personnel from obtaining network access. In emergency situations when wire line networks are damaged, cellular telephones often provide the primary means of communication, increasing congestion even further. In the year 2000, the Federal Communications Commission (FCC) issued a Report and Order (R&O) for Priority Access Service (PAS) authorizing wireless carriers to offer the service on a

voluntary basis and with much needed liability protections. Following the September 11 attacks, the White House directed delivery of a wireless priority service to persons with leadership responsibilities during emergency situations.

Highlights:

- WPS is an enhancement to basic cellular service that allows NS/EP calls to queue for the next available radio channel. The full WPS capability, which began deployment in early 2004, when used with GETS, should provide priority handling from the origination, through the network, to the called destination.
- WPS is invoked by dialing 272 prior to the destination number on cellular instruments that have been subscribed to the WPS feature.
- WPS costs are a one-time activation charge of no more than $10, a service fee of no more than $4.50 per month, and no more than a $.75 per minute usage fee for WPS (272) calls. These charges represent the maximum amounts charged by the cellular carrier and may be lower; contact your carrier for current rates.
- WPS is currently available nationwide in all of the AT&T Wireless, Nextel, and T-Mobile service areas that utilize GSM technology.
- Verizon Wireless and Sprint PCS are planning to offer WPS when modifications to their technology can be made, estimated for late 2006.

J. THE WORLD IS FLAT

According to Thomas L. Friedman, the world is flat because several technological and political forces have converged, and that has produced a global, Web-enabled playing field that allows for multiple forms of collaboration without regard to geography or distance - or soon, even language. We are no longer restricted by geographical boundaries or wire technology. Wireless technology like "steroids," pumped up collaboration, making it mobile and personal.

The DMIS Interoperability Backbone is a web service that provides responders with communication tools that allow them to share information with other responder organizations. Responder groups receive and transmit information over the web, enabling them to rapidly develop and exchange incident information with other responder organizations. This capability of sharing incident information gives all responders greater knowledge of a particular disaster event by leveraging technology to gain efficiency. This gained efficiency allows responders to:

- Gain Early Awareness
- Better Coordinate Response Among Organizations
- Save More Lives
- Minimize Property Damage

In addition, the Interoperability Backbone provides communication among all responder organizations that register with DMI- Services. NJDHSS and Navy Medicine will be able to share information and communicate with:

- Local Responder Organizations
- Statewide Responder Organizations
- Regional Responder Organizations
- National Responder Organizations
- Non-Governmental Responder Organizations

Any system that renders itself "DMIS-enabled" by developing its side of the interface to the DMIS Interoperability Backbone can share information with the DMIS Tools and with any other DMIS-enabled system "plugged in" to the Backbone. DMIS publishes the interface specifications used by external systems developers to "build their plug." Some systems have built their side of the interface in less than 2 weeks. DMIS tools and services are exposed to cooperating non-DMIS applications using open standards based Web-Services interfaces.

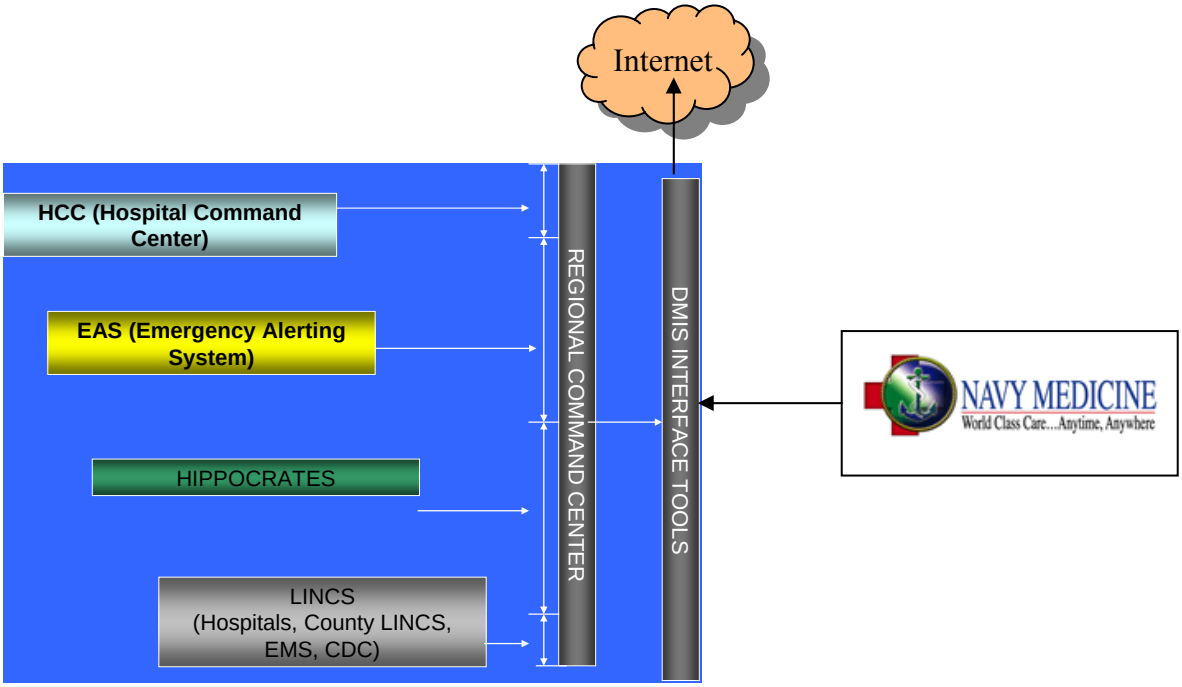


Figure 20. Proposed Infrastructure

Reliability of communications by either military or civilian personnel is a must. The ability to share information between military and civilian entities is very important. From the technologies researched my conclusion is that DMIS is the system of choice not only for the New Jersey DHSS but also for Navy Medicine as explained in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. NAVY MEDICINE SYSTEM

A. MEDICAL CAPABILITIES ASSESSMENT AND STATUS TOOL (M-CAST)

M-Cast applies specific and defined capabilities against requirements of program standards providing a standard measure of readiness for a given capability. Capabilities as viewed in this system represent smallest unit teams or squads performing specific functions required for a hazard type. While being applied to specific emergency management capabilities, the program standards have broader applicability to capabilities in general. Specifically, capabilities for response to chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) incidents should be measured against program standards and their objectives for an "all hazards" approach to emergency management. The lowest point at which threshold requirements of the standard are not met determines the level of "readiness" of a specific capability. Capability sets are grouped based on their level of criticality including "Baseline" assets (day-to-day functions), "Core" response capabilities (that must be "ready" and are measured and tracked), "Contingency" capabilities (that are task-organized to meet requirements from either baseline assets and core capabilities, or built during response to pre-set program standards), and "Reactionary" capabilities (that can be developed to meet extraordinary requirements). This information was released by BUMED for this thesis purpose; this information should not be release to other contractors since this contract has not been awarded as of today.

Core Group capabilities in compliance with the program standards are in a partial or fully "mission capable" status. The set of capabilities for a specific hazard response type (e.g., chemical attack) that are "ready" serve as a measure of "preparedness". "Responsiveness" measures the geospatial time factors from notification to mission ready. Deploy ability measures the ease of deploying, including factors such as weight and cube, ruggedness of gear, and logistical support requirements, and capability donor impact—the potential higher order effects on an institution by committing manpower,

equipment, and resources of that capability. Utility captures the combination of these factors and the impact to the donor, facilitating selection of the best available capabilities for a response.

Applied to hazard vulnerability assessments, critical infrastructure programs, and intelligence assessments, readiness and preparedness levels can provide information on vulnerability and be used to assess risk mitigated by having a capability, giving insight into capability effectiveness. Combined with cost, this allows determination of funding priorities for capability development. Through an iterative process, the tool can be vetted against local, regional, and national threat and hazard vulnerability assessments, adjusting the program standards or capability sets as needed to minimize risk.

Application of "lessons identified" from objective exercise assessments, or from evidence-based data collected from actual responses, and items from vulnerability assessments, form the basis for a continuous process improvement function. Analysis leads to changes in program management through adjustment of weighting factors applied to program standards and objectives, adding or deleting capabilities, adding or deleting objectives, adjusting readiness or preparedness thresholds, or refinement of the calculus for readiness and related qualities of the capabilities. Because capabilities are standardized and measured, metrics data and outcome data can be analyzed to isolate individual factors for their significance as the system matures. For example, the specific distribution of readiness scoring can be compared to lessons learned, outcomes, and identified measures of effectiveness in the process improvement function to identify specific factors that can be changed.

Operational risk management principles guide the use of capabilities to meet given requirements, based on readiness, responsiveness, deploy ability, and utility. These metrics and data can also provide significant insight into logistical support, time-phased force deployment data (TPFDD) requirements, and cost of response, as well as overall program management, and development of the common operational picture.

The National Response Plan (NRP) outlines further in detail the application of our national strategy for responding to incidents of national significance including roles and responsibilities of coordinating and cooperating agencies. Promulgation of a National

Incident Management System (NIMS) with its focus on integration and a national resource typing system has given a further detail to development of a standardized, systematic approach for a national response strategy. National Preparedness Goals seek to further refine this process. Identifying the complexities of the coordination, integration, and interoperability requirements and capturing them in information management tools that are useful becomes a challenge, akin to the beginnings of the construction of the "Borg" of Star Trek fame. Capturing all of the critical elements into a system requires recognizing the multidimensional, layered approach now capable of being managed only with elegant information technology tools. Without developing a systems architecture based on clearly defined and standardized objectives and requirements, such preparedness goals should not be met. Knowing where a response team is and what capability it is required to have is not sufficient. Readiness metrics must be defined, applied, and measured to those teams and considered carefully in order to perform necessary operational risk management decisions. In emergency management, using the available assets in developing and managing a response to given requirements requires knowing the current status of those assets and what the risk is in using the given capabilities across a "capabilities gap" to meet operational requirements.

The Medical Capabilities Assessment and Status Tool (M-CAST) provides a capabilities-based management system for task-organizing response teams for an "all hazards" emergency management program. It identifies critical program standards and indexes them against a range of capabilities grouped for specific mission or hazard type, organized in a matrix format (see Figure below). The technique is broadly applicable to any capabilities-based planning system, capturing critical elements through algorithms based on the standards and capabilities. A program standard is a defined objective that provides definition to meet the program requirements (After: MCAST Program).

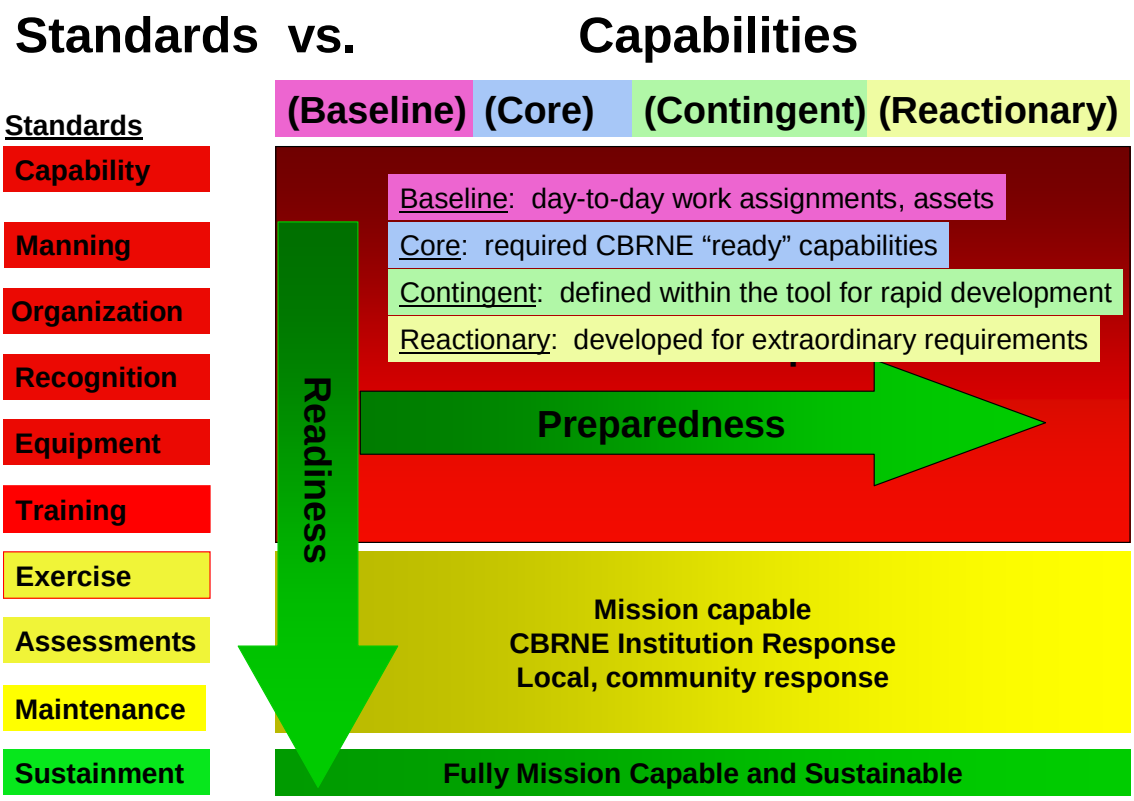


Figure 21. Standards (From M-CAST Program)

Objectives of the program standards provide further detail and definition. Rank-ordering the program standards properly provides a framework for measuring "readiness" for a given capability. Applying weighting factors to program standards and objectives provides a way to assign significance to specific elements (e.g., critical equipment, critical team members, critical training) that are identified as having greater impact on capability readiness. Summing up points of the product of weighting factor and score provides a "Readiness Factor", RF.

Capabilities represent the combination of properly equipped, trained, and organized personnel and assets ready to integrate into a response applied to given requirements. Functionally, they represent squads, teams, or units that perform the basic, elemental actions on an objective without any mixing or cross over of function. For example, a decontamination team does not perform triage or treatment of patients, only the decontamination function. These can be defined and standardized through a national

resource typing system or categorized through "unit type codes" for consistency across programs. As an individual capability meets more of the program standards, it achieves greater readiness and should have a higher readiness factor. Exceeding program standards is done so at the expense of the institution and does not qualify for extra credit in the readiness factor or more funds from a centrally managed program unless an exception or exemption is made. It would, however, be noted and visible to the system that additional capability exists. The capabilities are further divided into Capability Groups defined as "Baseline", "Core", "Contingency", and "Reactionary" depending on the determined effectiveness for a given capability. These groups then define the level of adherence required against the program standards, allowing optimal management under given fiscal constraints, as described below. Groups are divided into classes based on whether they are Hazard Specific, defining specialized capabilities for specific hazard types, or Functional, requiring coordinated actions across the entire institution. Types define the specific set of capabilities required for responding to such an incident.

As more capabilities achieve readiness, their sum capability provides greater "preparedness" for a given institution such that preparedness can be defined as the sum of capability readiness for a given capability set. Through checks, rights, and visibility, management at various layers within a hierarchical chain of command can provide oversight to accomplish critical tasks appropriate to that layer of management. Using warning flags and reports, deficiencies in meeting program standards allow real-time assessment of readiness and preparedness, better operational risk management decisions to be made, and a mechanism for measuring the effectiveness of program standards and capability definitions. Using the sustainment standard to capture cost, risk-based programming can help determine in which set a given capability should be placed.

For the purposes of this discussion, a response requirement represents a tasker, an implied or specified mission, or planned response assigned to an institution (e.g., military branch of service, a department, an installation, medical center, hospital, clinic, etc.), that owns or manages a capability.

1. Capability Classification Scheme

Capabilities for programs (e.g., Antiterrorism, Force Protection, and Emergency Management), local plans, operations, or functions (e.g., emergency support functions)

are designated in Groups defining their required level of preparedness. These should be *classified* further into Hazard Specific or Functional classes. These should then be *typed* into specific hazard or response Types (and sub-types) of capability sets to designate which capabilities are maintained, sustained, and subject to inspection, defined below.

Baseline Group—those skills, functions, or actions performed on a daily basis or with well established program oversight. These are governed by standards such as credentialing and privileging, licensing, certifications, etc., and include conventional mass casualty response capabilities that are based on everyday skills. Hazard specific class includes those that require very specific actions, are usually drilled in sections or covered in employee training, and are represented by the DoD standard color-coded types. Baseline Functional Types identify those that require broad participation or affect the institution on a broad scale. This includes the day to day operations and structure of departments, divisions, sections, and watches. Sub-types define those types that require further division to more manageable chunks. For example, C4ISR (command & control, communications, computer, intelligence, surveillance, and reconnaissance) would require sub-typing to more manageable pieces.

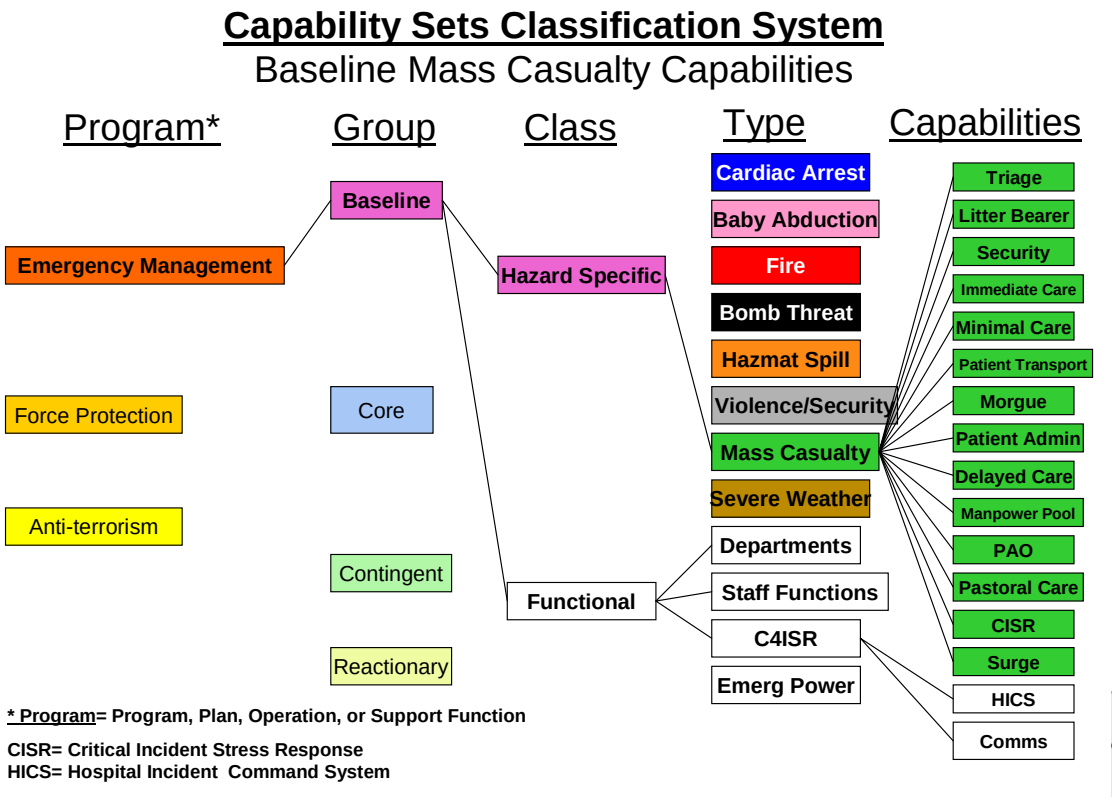


Figure 22. Capability Sets Classification System (From M-CAST Program)

Core Group--represent those capabilities that must be in a "ready" posture meeting the program standards defined by C MORE TEAMS, are subject to inspection, are used for planning and plans development including mutual aid agreements and memoranda of understanding, and remain visible to the hierarchical chain for overall readiness management, preparedness, planning, and response. Core group capabilities are further divided into either hazard specific classes or functional classes depending on whether they involve specific response elements or general, institution-wide response. These are further classified into specific types. Each type should consist of the set of capabilities organized at the team(s), squad(s), or unit level comprising that incident response capability. Those in the Core Group should be monitored by the flagging, warning, and reporting system (see below). For "Core CBRN" (chemical, biological, radiological, nuclear) such capabilities as "Triage and Treatment", "Medical Transport", "Decontamination", "Detection/ ID" are included and differentiated from non-CBRN sets due to the need for following additional statutory code and guidelines related to training

for and working in hazardous environments. These drive the need for specialized training and equipment such as personal protective equipment (e.g., chemical suits, gas masks, gloves, and boots), detection equipment, and decontamination equipment.

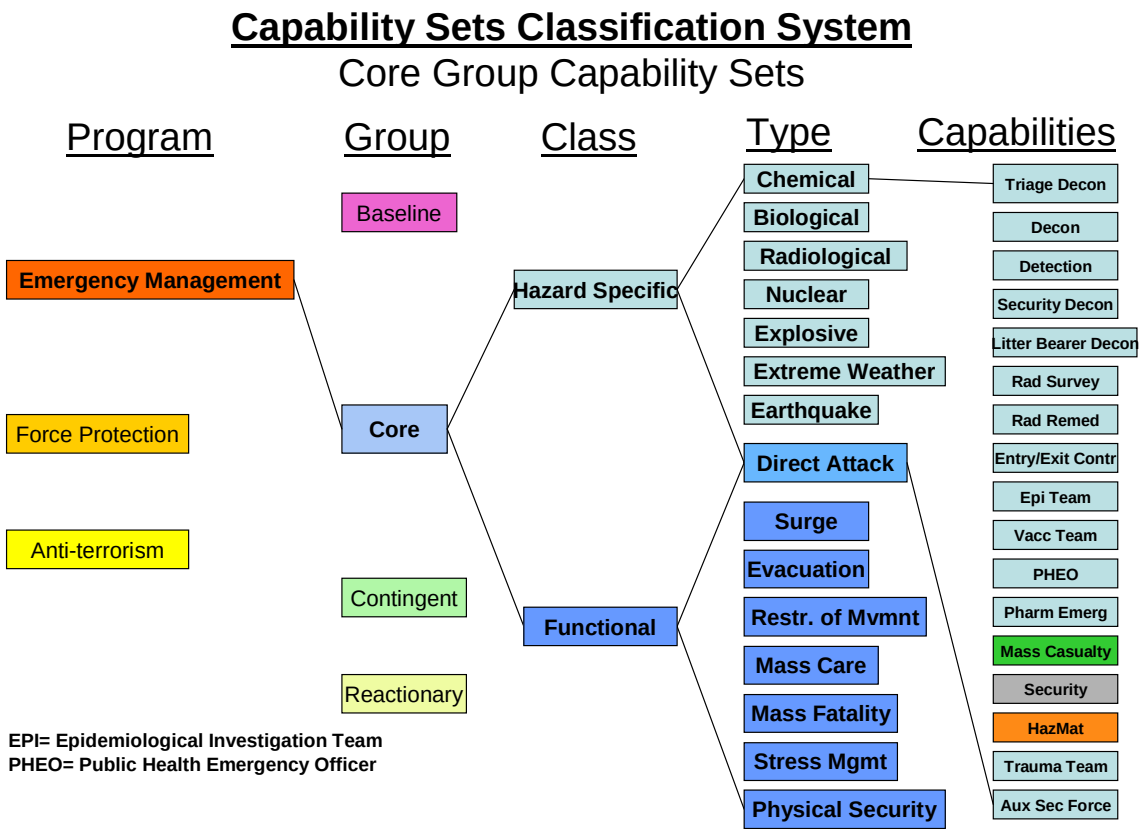


Figure 23. Classification System (From M-CAST Program)

Contingent Group—those capabilities that might be called upon to meet requirements of an incident response but either essentially meet program standards through other capabilities in the baseline and core sets, or are desirable capabilities to have, but not prioritized high enough to warrant funding. Contingent set capabilities are pre-defined and may be used for planning purposes in pre-incident phases; however, they do not require monitoring via the program standards until they are formed, are not subject to inspection, are not exercised, and are not funded. For example, baseline capabilities could be organized after an incident to meet requirements calling for specific medical capabilities such as surgical specialties, nursing, public health specialists, etc. where standards are based on their credentialed privileges, certifications, and/or qualifications.

While these would not require monitoring through the M-CAST program standards pre-incident, the tool would provide visibility for planning, team design to specified program standards, and accountability during response. Additionally, program standards and objectives promotes a more comprehensive consideration of ancillary requirements that may improve the "capability" (e.g., deploying technicians as part of a team, developing equipment lists for "go bags", selecting personnel with proper training, etc.). Below are Contingent Group Capability Types.

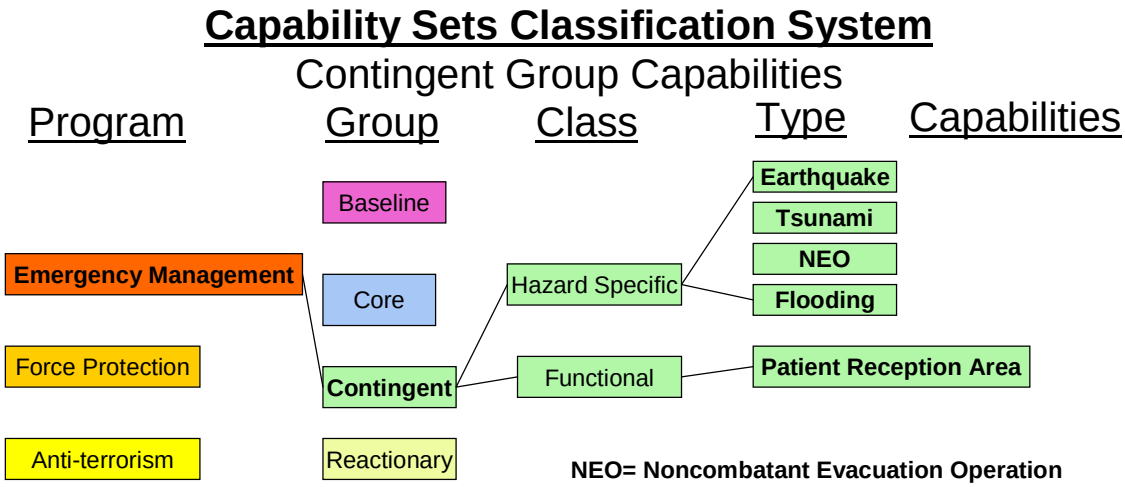


Figure 24. Capability Classification System (From M-CAST Program)

Reactionary Group—built essentially from baseline and core capabilities in response to a given incident, standards and objectives are defined through either local or central management on-the-fly, so that capabilities are developed around defined, minimal standards. Risk management provides opportunity to justify exceptions that are made in developing the capability and are documented in a risk assessment developed with assistance of the tool providing visibility on training, certifications, and experience of personnel, equipment sets, and impact to donating entities. Construction of the response teams to given program standards with appropriate visibility provided to planners, logisticians, and the chain of command should improve the common operating picture, streamline the deployment process, and improve the risk management for incident commanders.

2. Program Standards

The tool defines given capabilities against program standards captured in the acronym C MORE TEAMS©, (referring to the ability of the system to provide visibility on capabilities available in response and the ability to build more teams relatively easily).

- Capability is defined in local and higher level policy
- Manpower assigned by roster
- Organized within chain of command
- Recognized with horizontal integration, interoperability
- Equipped with approved/ certified equipment
- Trained and certified or qualified as needed
- Exercised with external entity
- Assessed with AAR and LL's feedback loop
- Maintained training and equipment program
- Sustained with ongoing funding

Objectives to the program standards should further define the characteristics of the capabilities, allowing for standardized, centralized resource typing according to current doctrine, policy, guidelines, and best practices. Variance from program standards is by exception or allowance. The tool should allow for updates and changes as they occur by making changes in the programs standards and objectives. It also should alert managers as to specific areas impacted by those changes through an embedded warning, reporting, and flagging system (see below). Capabilities and resources should be defined in accordance with the national resource typing system described in the NIMS where available. The controls in the program standards define the limits of decentralization of decision making authority and can be updated as dictated through a continuous quality improvement process and evolution of the tool. Appendix B lists current capability standards definitions.

Capability captures policy, scope, purpose, mission, and basic concept of operations for a given capability requirement. In the final form, hyperlinks provide immediate access to pertinent references requiring a given capability and the objectives. Links to institutional level plans describe where specific capabilities should be employed at the institutional (and/or installation) level.

Manning provides the roster of personnel, including alternates, with pertinent associated information allowing for logistical support, personnel accountability, "readiness" (in the military this includes things like "C-status"), and data for development of time phased force deployment data (TPFDD). Position Descriptions designate key positions, to include the team or squad leader, assistant, supply manager, training manager, equipment manager, maintenance manager, and any unique positions required for a given capability. Depending on the size of the team or squad, or the responsibilities, members may hold more than one position. Line of succession is also designated by the roster numbering scheme. Personnel may be on more than one capability, but must meet training requirements for all on which they are listed, and must be substituted if conflicts are identified between capability employments. Algorithms should determine which capabilities represent potential or absolute conflicts and should not designate the same personnel (e.g., a person should not be assigned to a decon team and triage team for chemical incident mass casualty response) and should be flagged or disallowed. Appropriate personnel data should be pulled from the appropriate administrative databases able to provide the required data fields. Read and write rights should be determined to prevent inappropriate access to personal data (see below). Manning rosters should be linked to training files with the appropriate training records for an assigned capability visible. Accountability data should provide biographical identification capability to ensure compliance with Antiterrorism (AT) and Force Protection (FP) Program standards. Visibility of institution personnel with respect to readiness and training status should aid in filtering of the available manpower pool for assignment of properly trained and equipped team members.

Organization defines the command and control within the incident management system including vertical integration and reporting requirements, or operational chain of command (CoC). It also includes the administrative and tactical chains of command, if separate from the operational CoC, and hierarchical management, communications protocols, and succession plan.

Recognition comprises horizontal integration and interoperability issues--how given capabilities interface with other capabilities, capturing those issues in terms of, for example, sharing of equipment, command and control, communications, oversight,

operational authority, chain of custody, and continuity of care (for example, who has medical oversight of patients through the decontamination process when there may be no medical providers on the decontamination team). Tactics, techniques, and procedures (TTP) are maintained here. Check lists of critical action items for personnel associated with the capability, including the job action sheets of the Hospital Incident Command System (HICS), are maintained here and updated based on assessments and as needed. As an example, the integration of the formal decontamination capability with the triage and treatment capability establishes such protocols as medical oversight of patients through processes, intervention procedures, patient hand-off techniques and responsibilities, and command and control. Mutual aid agreements (MAA), Memorandum of Understandings (MOU), and Memorandum of Agreements (MOA) are referenced and copies maintained here.

Equipment and supply lists specific equipment and supply lists for given capabilities either as the specific list or as a family of systems from which to choose. Communications gear and plans are noted here, cross-linked with the protocols in the Organization Program Standard. Minimum standards are promulgated for inspection purposes, and deviation is by exception from proper authority as designated within the specifics of the program. Actual equipment and supplies on hand with proper storage location, condition, and status are captured here. Comparison is made against the specified equipment list or family of systems, with deviations and exceptions noted in the tickler, warning, and reporting system (see below).

Training is determined by minimum standard requirements as designated by a given program's requirement or standard and recorded as "qualified" for a given skill. This qualification has sustainment training requirements that must be met. It also qualifies this person system-wide as long as it is maintained. For example, Occupational Safety and Health Administration (OSHA) and National Fire Protection Association (NFPA) provide minimum training standards for first responders, first receivers (guidelines), and hazardous materials workers and likely provide the minimum standard for "certification" or "qualification" purposes. Minimum standards are determined for a given manning position, as is sustainment, advanced, and expert (train the trainer) level training. Training data pulled from appropriate databases should compare completed

training to training requirements for the role being filled and note deficiencies. Credentialing and privileging information should be included in accordance with appropriate requirements. Training is also cumulative and cross applicable, such that training for one capability may be applicable towards the training requirements of other capabilities. This allows managers to identify specific training (such as specific equipment training) that can be done easily to expand the potential personnel assets for various capabilities. Relative Value Units (RVU's), which capture equivalency time for training against that for clinical time, should be captured and appropriately coded for a given capability such that specific capabilities requiring more training should reflect the number of RVU's required. On-the-job training during actual incidents should be at the discretion of managers with the appropriate expertise and experience after making the proper risk assessment.

Exercises are recorded in terms of duration, frequency, participation, and goals. Duration captures time spent during exercises and counts towards practical application training requirements for qualification and/or certification purposes. Frequency is determined by program standards, again established by the most stringent requirements to which the institution adheres. For example, medical institutions adhering to Joint Commission on Accreditation of Healthcare Organizations (JCAHO) standards would schedule to meet those exercise requirements even if they exceeded higher authority military requirements. Participation includes all capabilities exercised with annotation of outside organizations included for interoperability purposes. Goals shall include itemized issues for action from previous assessment lessons identified that are to be assessed and are included in the exercise master event scenario list (MESL), designed to test components of universal task list (UTL), a standard list of tasks responders in specific positions must be able to accomplish. Military service specific requirements at the installation and/ or regional level would be factored into the exercise goals. Various other programs of record might also drive the frequency, duration, participation, or goals (e.g., Emergency Management Program, CBRNE Installation Preparedness Programs, Anti-terrorism/ Force Protection Programs, or Critical Infrastructure Programs, and may do so at various hierarchical levels (e.g., installation, regional, headquarters).

Assessments of training, exercises, and inspections are captured as a formal program standard and are submitted in the form of After Action Reports (AAR) or Lessons Identified, and are used to develop, evaluate, modify or validate program standards and objectives for the capabilities. These are entered into a formal continuous quality improvement program ensuring they are reviewed, with issue items assigned as action items with designated personnel charged to address them within a given time frame, and recorded for later inspection. These are then included in the next exercise master event scenario list (MESL) for evaluation during the next exercise. Review is also conducted at the central headquarters level by an MCAST oversight committee to incorporate changes into the tool and transition lessons identified to Lessons Learned through a formalized mechanism. Lessons learned are then documented with date/time group, rationale, and associated change to the system (see below). A lesson identified is not a lesson learned until it has been processed completely through the formal continuous improvement process and an outcome designated.

Maintenance refers to equipment and supply storage management. Each capability with equipment has an assigned maintenance manager and equipment manager charged with ensuring proper maintenance is conducted, and proper storage maintained. Maintenance schedules are tied to the tickler, warning, and reporting system. Availability (Ao): Operational availability is calculated as Ao = Mean Time Between Maintenance ÷ (Mean Time Between Maintenance + Mean Down Time which includes Logistics Delay Time, Admin Delays and Mean time To Repair). Training maintenance is maintained by the training manager and reflected there; however, costs are rolled up under the Maintenance Program Standard.

Sustainment of the program through proper budgeting for adherence to program standards must be demonstrated. This includes operations and maintenance funding, equipment life-cycle replacement costs, supplies, training, exercise, and assessment costs including relative value unit (RVU) costs. Sustainment figures are used in risk-based cost benefit analysis for capabilities as well as for estimates of logistical support during operations. Figures should include actual costs to sustain a given capability, and may include notional cost estimates to sustain a capability through various program standards to allow for visibility on cost for a given level of readiness.

3. Layers of Management

The tool can be used by managers at various layers of the incident management system recognizing that an overall hierarchy must merge disparate command systems' data supporting the incident. The system must account for hierarchical administrative, operational, and tactical command chains. Table 3 demonstrates a 7 layer model (with sub layers) which identifies key management layers and roles within the incident management system. Such a model provides general visibility on layers of management for development of chain of command, hierarchical structure, write/read rights for data input, responsibility for veracity of that data, and action requirements within the program standards. Each capability is defined across these layers, as appropriate, with as specific as possible definition of the key position or billet with respect to management requirements, reporting structure, and write/read rights. Administrative, operational, or tactical command chains are so designated.

Layer	**Management entity**	**Leader element (DoD equivalent title)**
Layer 7	Federal/ General/ Other	Secretary (NORTHCOM, OSD, COCOM)
Layer 6	Regional/ State	Governor (Service HQ, JRMPO, JTF-CS)
Layer 5	Local EOC	Mayor (Installation CO)
Layer 4	Incident Command Post	Incident Commander
Layer 4a	Sections	Section Chiefs
Layer 3b	Branch	Branch Level Managers
Layer 3a	Division/ Group	Supervisor
Layer 2	Unit/ Squad/ Team/ Task Force	Leader
Layer 1	Single resource	First Responder/ Receiver

Table 3. Layer Model for Incident Command Structure.

The below Figure demonstrates similar information in wire diagram form. It does not include Layer 1, single resource "first responder/ first receiver", or Layer 7 at the national level.

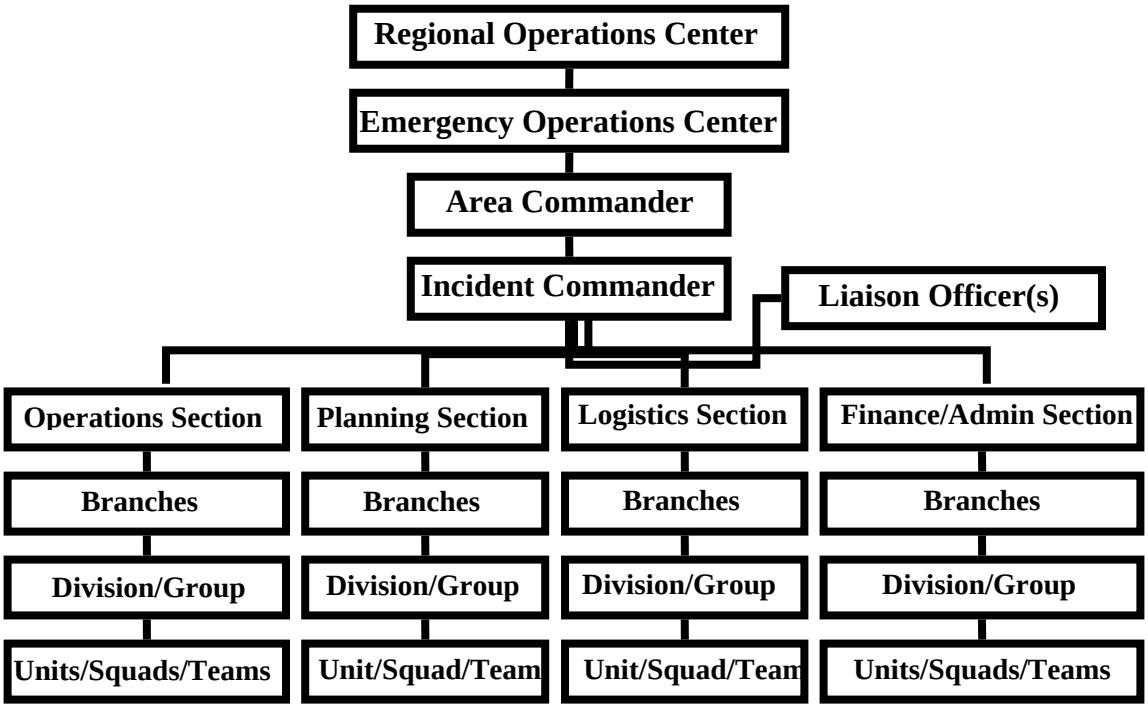


Figure 25. Wire Diagram (From: M-CAST System)

Common Operating Picture is promoted by providing the necessary visibility at the various layers of the hierarchical command system. Critical data is determined by the functions, roles, and responsibilities of various positions within each of the layers. Access to data is pre-determined and dashboard views customized for the given layers. Figure 26 demonstrates employment of M-CAST across a hierarchical enterprise, emphasizing some of the key functions at the various layers of management.

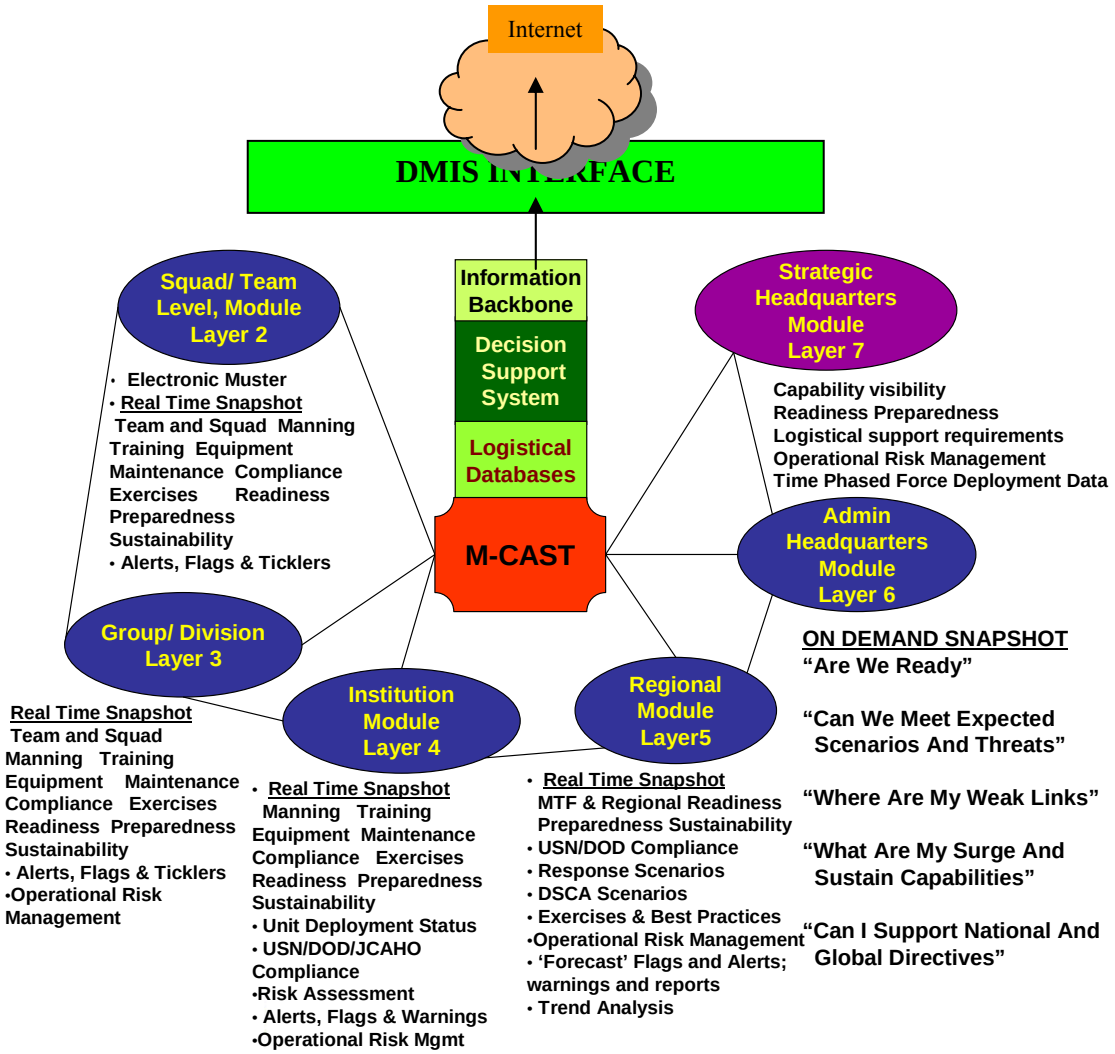


Figure 26. Common Operating View (After: M-CAST Program)

Reliability of communications by either military or civilian personnel is a must. The ability to share information between military and civilian entities is very important, below is a diagram that shows how the military and civilians would interact in case of emergencies.

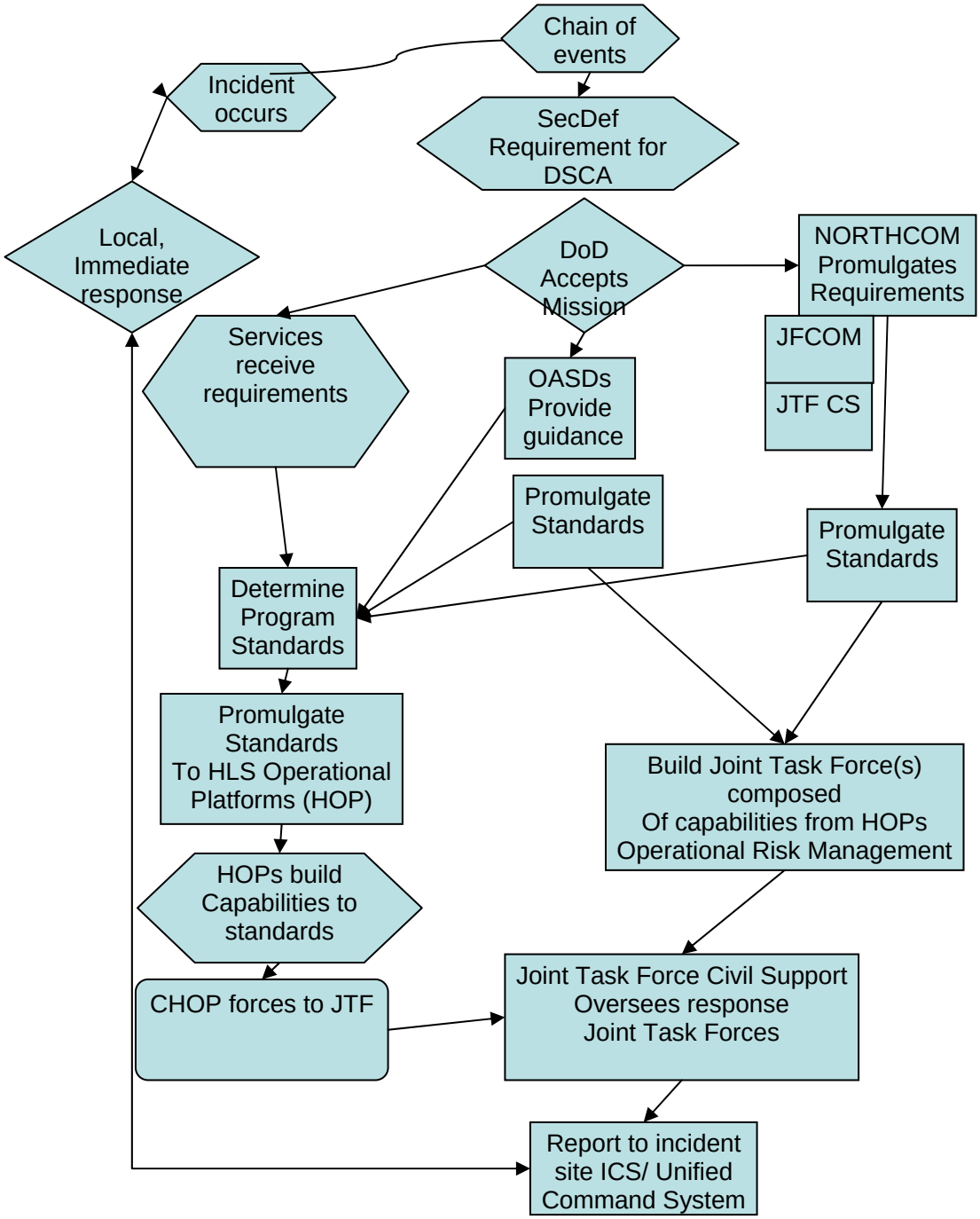


Figure 27. Military Respond flow Diagram

IX. CONCLUSION

The best business practice call for a workflow representation of action plans for crisis management. Using workflows that can adapt schemes for the establishment of virtual enterprises to the discovery and integration of appropriate emergency services personnel for a given crisis management plan.

From the research I have accomplished, I would advocate that the New Jersey Department of Health and Senior Services look into the DMIS System solution. As we have seen most responders report enclaves or "islands" of good information sharing within certain organizations but generally very little capability to share digital information among mutual aid partnerships or between civilian and military support organizations to include NJDHSS.

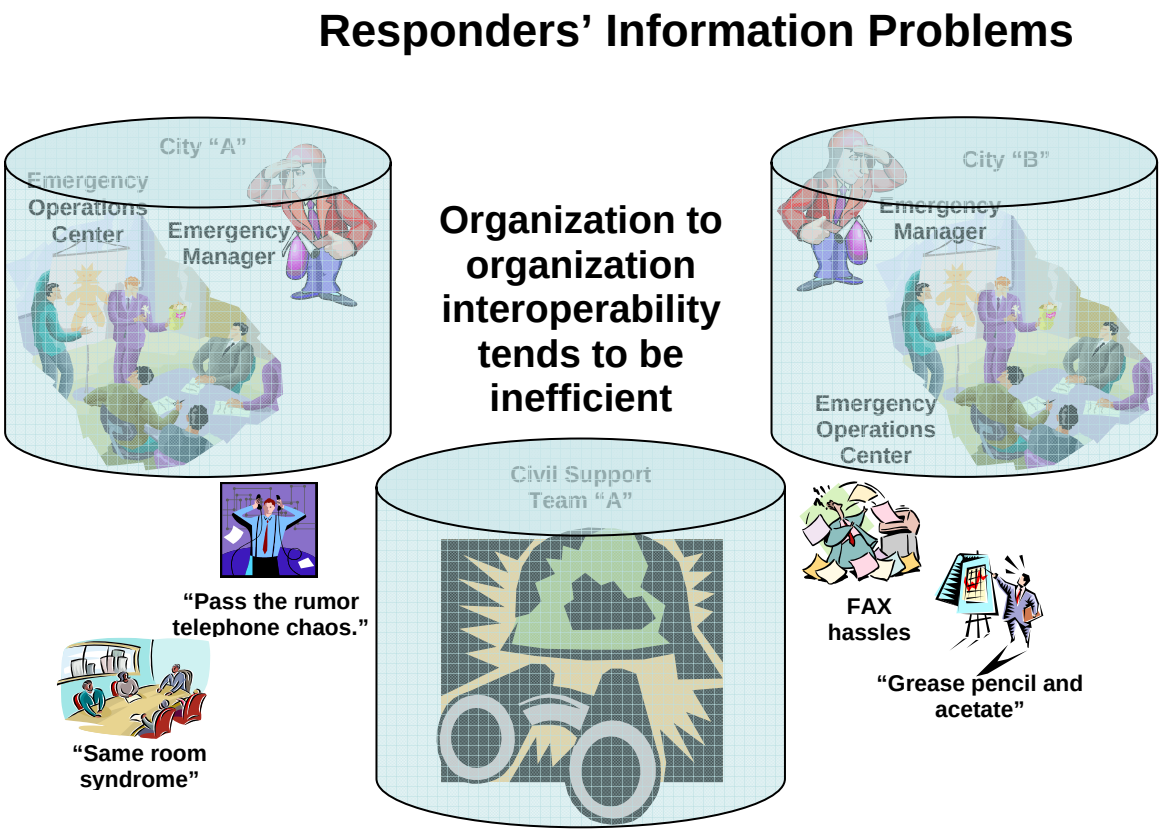


Figure 28. Responders Information Problems (Source: DMIS)

From its inceptions, DMIS solution was to have an interoperability platform and a set of basic tools. The interoperability backbone is one of the most important aspects of DMIS. It is the backbone that allows responders to acquire software that best suits their needs without having to worry about their neighbors buying the same software. The backbone enables information sharing among all systems that develop an automated program interface to it. In addition the basic tools provide responders with the basic ability to describe an incident and request specific needs.

In order to leverage technology and gain efficiency DMIS has developed a national emergency information interoperability service enabling horizontal and vertical data sharing.

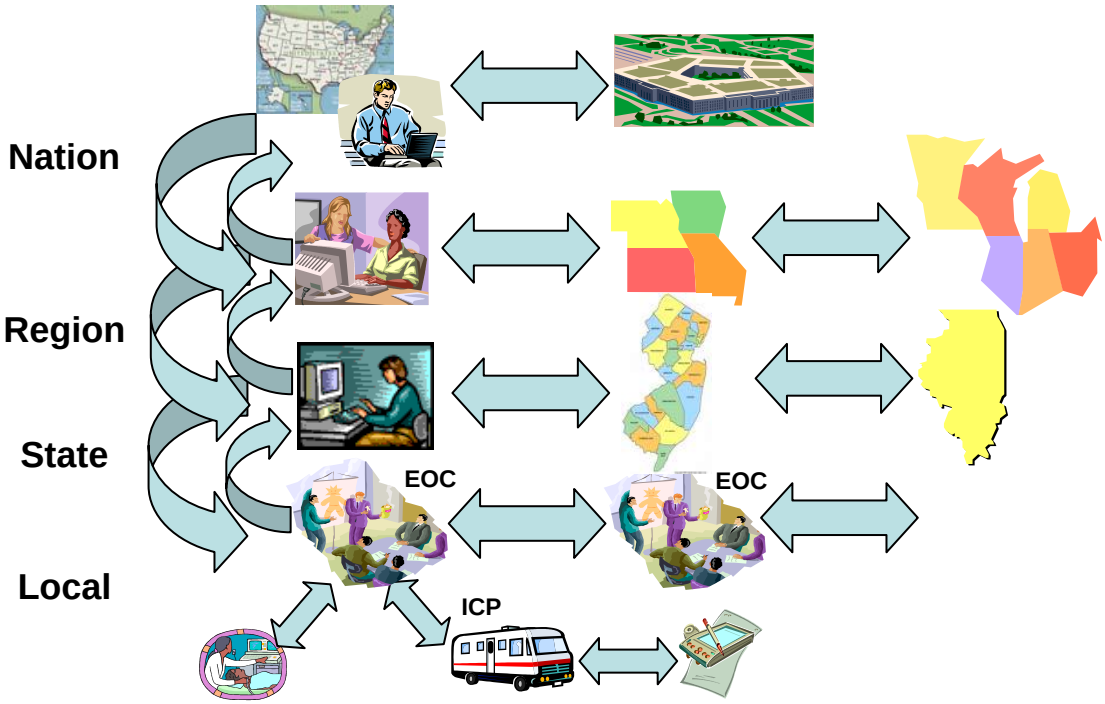


Figure 29. Horizontal and Vertical Data sharing Flow

In addition the Emergency Management Technical Committee consists of government and commercial members working together to formally develop standards facilitating interoperability. DMIS implements the standards quickly and includes them in the published DMIS backbone interface specification. This provides software companies with a “hard engineering target” for developing their side of the DMIS

backbone interface. A key to reaching higher levels of interoperability maturity is the resolution of subtle differences in data definitions among various systems. Currently, the DMIS Backbone and DMIS Tools are used most commonly in Emergency Operations Centers at local, mutual aid partner, state, regional, and national levels. There are a few jurisdictions experimenting with the use of DMIS at the Incident Command Post. Those jurisdictions have the resources to 56 KBPS (or faster) wireless data connections "to the street." From the national viewpoint, DMIS is used in over 1400 operating groups in all 50 states (DMIS Report).

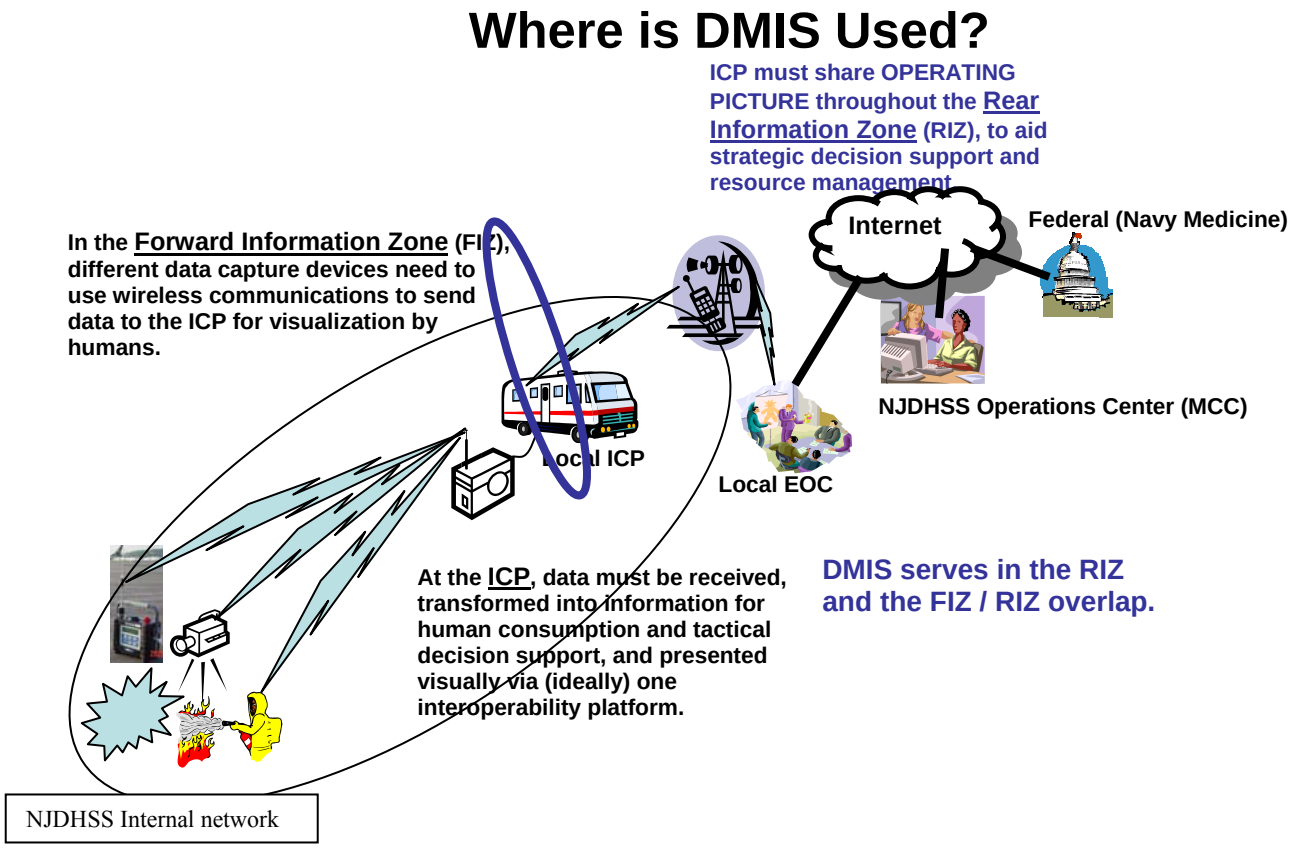


Figure 30. DMIS Operations (From: DMIS)

DMIS tools will help NJDHSS and Navy Medicine because they provide the ability to describe an incident and make specific needs requests in enough detail for shared situation awareness with other organizations that may be called upon to help. Within the Tactical Information Exchange (TIE) portion of DMIS, there are information

forms that are named and look like the acetate-covered information boards in traditional

Emergency Operations Centers. Locatable incident information (such as the incident site, hospitals, shelters, etc.) entered into the TIE forms may be automatically plotted on the incident map.

The map is central to providing and sharing the "common operating picture" of the incident or situation. Specific Needs Request (SNR) enables listing of needs by local responders. Other organizations can respond to the requests by articulating what assets they could provide.

The DMIS Messenger is a private online "chat" capability responders can use to communicate with other DMIS members real time. All DMIS Operators who have DMIS Messenger running are available to be invited to join a chat session.

DMIS Alerts provide the ability to quickly broadcast critical information to DMIS Operators in CAP standard format. Alerts are available as a stand-alone tool in DMIS or from within the TIE subsystem.

The National Summary Map is used to display incidents with the notification level of "National." This is a valuable tool for those at higher levels of Government to see an overview of incidents in progress around the country.

The Weather Forecast tool may be accessed within the TIE subsystem or via the Disaster Management Tools menu. DMIS currently enables users to enter a ZIP code and obtain AccuWeather forecast data, in one-hour increments, for the next 48 hours. The user may choose to convert the data for the current hour into a weather observation for a working incident record in TIE. Weather observations may also be entered in the TIE Weather Observations form directly

In addition there are key principles that characterize DMIS. DMIS is built "from the bottom up" in recognition of the fact that all disasters – no matter how consequential or large-scaled – are first encountered by local responders. DMIS is designed to capture the local situation and share it with those with the need to know. And the map is the central means of depicting that situation. DMIS seeks to "use the data where it lies." For example, it is easy to use a national data source for aerial photograph layers over maps (orthoimages). But those orthoimages are generally older than those available at state

and local level. DMIS has adopted an open interface standard that will make it relatively easy for responders to use more "local" data to locate items on a map.

Although NJDHSS is very adamant to use their "own" system; the good news is that DMIS allows external systems to use DMIS access control services to make sure that only legitimate responders are using the system of systems. There are several common services exposed through the interface that are necessary to manage information transactions among the participating external systems. The DMIS Alert function is also freely available, as an option, to external systems who build an interface to the DMIS Backbone. When external systems package an incident report and use the DMIS Post function within the interface, a DMIS incident record is automatically generated for dissemination via the DMIS backbone. The Attach function within the interface allows external systems to attach files to Alerts and Incident Records for sharing with others via the Post function.

Hippocrates is obviously to be optimized for the health service domain. That poises it to be a "summary data feeder" to the broader all-hazards incident management systems – a very good thing. I would advocate that NJDHSS employs an open interoperability backbone enabling data sharing to all hazards incident management systems. Suggest starting with CAP. While created for the alerting function, it can also be inappropriately but practically used as a general text message among heterogeneous incident management systems.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] GAO-02-621T, "National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security," April 2002

[2] Bowman, S., Kapp, L., Belasco, A., & Library of Congress. Congressional Research Service. (2005). Hurricane Katrina [electronic resource] : DoD disaster response. Washington, D.C: Congressional Research Service, Library of Congress. from http://library.nps.navy.mil/uhtbin/hyperion/CRS-RL33095.pdf May 2006

[3] Broder, J. M., Wald, Reporting for this article was contributed by Matt, Miami, T. A. i., Reuthling, G., & Zezima, K. (2005, Sep 25). In plans to evacuate U.S. cities, chance for havoc. New York Times, p. 1.1.

[4] Carlson, C. (2005). Agencies under fire for disaster recovery plans; comparing the potential effect of a cyber-disaster to the ravages of hurricane Katrina, lawmakers have called on the department of homeland security and commercial infrastructure owners to explain why more progress isn't evident in preparing for a massive cyber-attack. EWeek, 22(38), 37.

[5] Guyette, J. E. (2005). Preparing for disaster. LP - Gas, 65(10), 24. Hernandez, N. (2005, Sep 30). Navy hospital creates A theater of terror; emergency workers run disaster drill. The Washington Post, p. B.03.

[6] Johnson, E. K., Paton, B. H., Threat, E. W., Haptonstall, L. A., & Naval Postgraduate School (U.S.). (2005). Joint contingency contracting. (Doctoral dissertation, Naval Postgraduate School). , 148. (Springfield, VA. : Available from National Technical Information Service)

[7] King, R. O., & Library of Congress. Congressional Research Service. (2005). Federal flood insurance [electronic resource] : The repetitive loss problem. Washington, D.C: Congressional Research Service, Library of Congress. from http://library.nps.navy.mil/uhtbin/hyperion/CRS-RL32972.pdf May 2006

[8] Lombardi, K. S. (2005, Sep 18). Gathering, between tragedy and peril. New York Times, p. 14WC.1.

[9] Morrissey, W. A., & Library of Congress. Congressional Research Service. (2005). Tsunamis [electronic resource] : Monitoring, detection, and early warning systems. Washington, D.C: Congressional Research Service, Library of Congress. from http://library.nps.navy.mil/uhtbin/hyperion/CRS-RL32739.pdf June 2006

[10] Petersen, R. E., & Library of Congress. Congressional Research Service. (2005). Emergency preparedness and continuity of operations (COOP) planning in the federal judiciary [electronic resource]. Washington, D.C: Congressional Research Service, Library of Congress. from http://library.nps.navy.mil/uhtbin/hyperion/CRS-RL31978.pdf June 2006

[11] Romano, M. (2005). At capacity and beyond. Modern Healthcare, 35(39), 6. Sauter, M., & Carafano, J. J. (2005). Homeland security : A complete guide to understanding, preventing, and surviving terrorism. New York: McGraw- Hill. from Table of contents http://www.loc.gov/catdir/toc/ecip055/2004030511.html May 2006

[12] Tsou, W. (2005). Hurricane tragedy offers lessons for public health preparedness. The Nation's Health, 35(8), 2.

BIBLIOGRAPHY

http://www.bt.cdc.gov/ May 2006
CDC Bioterrorism Preparedness and Response Program
The Bioterrorism Preparedness and Response Program at the CDC is devoted to coordinating a public health response to a bioterrorist attack. This web site provides information about chemical and biological agents, press releases, training, contacts, and other important information relating to the public health aspects of bioterrorism preparedness and response.

http://www.apic.org/bioterror June 2006
APIC/CDC Bioterrorism Readiness Plan: A Template for Healthcare Facilities Prepared by the Association for Professionals in Infection Control and Epidemiology (APIC) Bioterrorism Task Force and the CDC Hospital Infections Program Bioterrorism Working Group, this document is intended to be used as a reference tool for infection control (IC) professionals and healthcare epidemiologists in the development of practical and realistic response plans for healthcare facilities in preparation for a real or suspected bioterrorist attack.

ftp://ftp.cdc.gov/pub/Publications/mmwr/RR/RR4904.pdf December 2005
Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response – Recommendations of the CDC Strategic Planning Working Group *MMWR*. 2000; 49: RR-4.
Prepared by the CDC Strategic Planning Group, this strategic plan contains recommendations to reduce U.S. vulnerability to deliberate dissemination of biological or chemical agents by addressing the role of public health in preparedness planning, detection and surveillance, laboratory analysis, emergency response, and communication systems.

http://www.hopkins-biodefense.org April 2006
Johns Hopkins University Center for Civilian Biodefense Studies. The Johns Hopkins University Center for Civilian Biodefense Studies is a part of the Johns Hopkins Schools of Medicine and Public Health. The Center aims to raise consciousness and knowledge base regarding the medical and public health threats posed by biological weapons, and to foster the planning and preparation for response to possible bioterrorist attacks. This web site provides
New Jersey Department of Health and Senior Services (NJDHSS) Bioterrorism Surveillance and Epidemiologic Response Plan

http://www.cdc.gov/ncidod/eid/vol5no4/pdf/v5n4.pdf December 2005
The Journal of Emerging Infectious Diseases.1999;5(4): 491-592.
The Journal of Emerging Infectious Diseases is a peer-reviewed journal published by the National Center for Infectious Diseases of the CDC. This volume of EID is largely devoted to issues related to biological warfare.

http://ccc.apgea.army.mil/Documents/HandbookonBioCas/Handbook.htm December 2005
US Army Medical Research Institute of Infectious Diseases (USAMRIID) Medical Management of Biological Casualties Handbook Published by the USAMRIID, the purpose of this Handbook is to provide concise supplemental reading material to assist in education of biological casualty management. The handbook contains information on biological agents, diagnosis, treatment, and prophylaxis.

http://chemdef.apgea.army.mil/ November 2005
USAMRICD – U.S. Army Medical Research Institute for Chemical Defense
The U.S. Army Medical Research Institute for Chemical Defense is devoted to developing medical countermeasures to chemical warfare agents and to train medical personnel in the medical management of chemical casualties. This web site provides information about training, published materials, and links to other web sites about chemical terrorism, including a link to the Textbook of Military Medicine Medical Aspects of Chemical and Biological Warfare.

http://cns.miis.edu/ October 2005
Center for Nonproliferation Studies, Monterey Institute for International Studies
The Monterey Institute is the world's largest non-governmental organization devoted to combating the spread of WMD. Web site materials, authored primarily by the Institute, are organized by geographical region, publication type, and subject (chemical and biological weapons, missiles, nuclear weapons, and treaties and regimes).

http://www.stimson.org/cwc/index.html October 2005
The Henry L. Stimpson Center Chemical and Biological Weapons Nonproliferation Project The Chemical and Biological Weapons Nonproliferation Project of the Henry L. Stimson Center examines the panoply of issues associated with chemical and biological weapons, including treaties for threat control and reduction, weapons destruction technologies, and export controls. This web site offers materials developed specifically for the project, and is organized by geographical region and subject.

http://www.gao.gov/new.items/he00180.pdf October 2005
West Nile Virus Outbreak: Lessons for Public Health Preparedness.
The General Accounting Office (GAO) is the investigative arm of Congress. GAO examines the use of public funds, evaluates federal programs and activities, and provides analyses, options, recommendations, and other assistance to help the Congress make effective oversight, policy, and funding decisions. This report reviews the local, state, and federal public health response to the 1999 West Nile Virus Outbreak.

http://www.mssny.org/pub_health/Emergency_Primer.htm October 2005
The Medical Society of the State of New York. Public Health Emergencies:
Quick Primer for Clinicians on Detecting Public Health Emergencies.

http://www.nysemo.state.ny.us/ICS/explain.htm December 2005
The New York State Emergency Management Office
This web site contains information about the Incident Command System (I.C.S) and the Standardized Emergency Management System (S.E.M.S.).

Bioterrorism-related published works:

Alibek K, Handleman S. Biohazard. New York, NY: Random House; 1999.

Arnon SS, Schechter R, Inglesby TV, et al. Botulinum Toxin as a Biological Weapon: Medical & Public Health Management. *JAMA. 2001;285:1059-1070.*

Bioterrorism Alleging Use of Anthrax and Interim Guidelines for Management United States, 1998. *MMWR*. 1999; 48(04): 69-74.

Chin J, ed. Control of Communicable Diseases Manual. Washington DC: APHA; 2000.

Christopher GW, Cieslak TJ, Pavlin JA, Eitzen EM. Biological Warfare: A Historical Perspective. *JAMA*. 1997; 278: 412-417.

Fine A, Layton M. Lessons from the West Nile Viral Encephalitis Outbreak in New York City, 1999: Implications for Bioterrorism Preparedness. *Clinical Infectious Diseases.* 2001;32:277-282.

Frantz DR, Jahrling PB, Friedlander AM, et al. Clinical Recognition and Management of Patients Exposed to Biological Warfare Agents. *JAMA*. 1997; 278:399-411.

Guillemin J. Anthrax: The Investigation of a Deadly Outbreak. Berkeley: The University of California Press; 1999.

Henderson DA, Inglesby TV, Bartlett JG, et al. Smallpox as a Biological Weapon: Medical & Public Health Management. *JAMA. 1999;281:2127-213.*

Henderson DA, Inglesby TV, O'Toole T. Implications of Pandemic Influenza for Bioterrorism Response. *Clinical Infectious Diseases*. 2000;31:1409-1413.

Hoffman RE, Norton JE. Lessons learned form a full-scale bioterrorism exercise. *The Journal of Emerging Infectious Diseases*.1999; 6(6): 652-653.

Inglesby TV, Henderson DA, Bartlett JG, et al. Anthrax as a Biological Weapon: Medical & Public Health Management. *JAMA. 1999;281:1735-1745.*

Inglesby TV, Henderson DA, Bartlett JG, et al. Plague as a Biological Weapon: Medical & Public Health Management. *JAMA. 2000;283:2281-2290*

Khan AS, Morse S, Lillibridge SR. Public-health preparedness for biological terrorism in the USA. The Lancet. 2000; 356:1179-1182.

Lederberg J, ed. Biological Warfare: Limiting the Threat. Cambridge: The MIT Press; 1999.

Meselson M, Guillemin J, High-Jones M, et al. The Sverdlovsk Anthrax Outbreak of 1979. *Science*. 1994; 266:1202-1208.

Zajtchuk R, Bellamy RF, eds. Textbook of Military Medicine: Medical Aspects of Chemical and Biological Warfare. Washington DC: Office of the Surgeon General, US Department of the Army; 1997.

State of California Documents:

The State of California Emergency Plan. Governor's Office of Emergency Services. May, 1998.

The Local Planning Guidance on Terrorism Response: A Supplement to the Emergency Planning Guidance for Local Government. Governor's Office of Emergency Services. December, 1998.

The California Terrorism Response Plan: An Annex to the State Emergency Plan. Governor's Office of Emergency Services. March, 1999.

California Influenza Pandemic Response Plan. California Department of Health Services, Division of Communicable Disease Control, Immunization Branch. May, 2000.

Other bioterrorism-related documents:

Public Health Screening at U.S. Ports of Entry: A Guide for Federal Inspectors.

U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Center for Infectious Diseases, Division of Quarantine.

APPENDIX A. INFECTIOUS DISEASE EMERGENCY PLAN

A. BASIC PLAN

This plan is based on the California Infectious Disease Emergency Plan. The NJDHSS, New Jersey', Infectious Disease Emergency Plan (IDEP) should mirror the California's IDEP. The plan was sent to the New Jersey Department of Senior Services but we have not received any feedback as of today. The project has been temporarily put on hold. This plan should help to assist the NJDHSS and its cities and towns in their preparedness activities to respond to an infectious disease emergency, such as an influenza pandemic or bioterrorism agent release, in order to minimize morbidity and mortality, and maintain health care and other essential community services during periods of high absenteeism due to illness.

This IDEP has been specifically designed to serve as an Annex to their Comprehensive Emergency Management Plan (CEMP) and supplements that document. Every effort should be made to integrate the IDEP with the CEMP. In that regard, the IDEP is consistent with existing authorities, planning assumptions, systems and procedures.

1. Objectives

The objectives of the NJDHSS and Infectious Disease Emergency Plan are to:

1. Describe courses of action that should minimize morbidity and mortality from an outbreak of infectious disease.
2. Establish procedures to provide for a coordinated effort among cities and towns in response to an infectious disease emergency.
3. Identify emergency response organizations, facilities and other resources that can be utilized during an outbreak of infectious disease.
4. Provide a mechanism to integrate community and facility response procedures.

B. ASSUMPTIONS UPON WHICH IDEP IS BASED

1. Assumptions: Infectious Disease Emergency

1. Infectious disease emergencies are inevitable.

2. In the event of an infectious disease emergency, local officials, the healthcare community and the general public should look to the local health department to coordinate the response.

3. There should be widespread circulation of conflicting information, misinformation and rumors. Communication must be coordinated among all relevant agencies to ensure consistent messages to all entities involved in the response and to the general public.

4. The infectious disease emergency must take priority until the emergency is resolved.

5. Even during a minor event, such as a case of hepatitis A in a food handler or one case of measles on a college campus, local health departments should be responsible for coordinating the distribution and/or administration of vaccine and other relevant pharmaceuticals in their jurisdiction.

2. Assumptions: Influenza Pandemic

1. An influenza pandemic is inevitable.

2. There may be very little warning. Most experts believe that we should have between one and six months between the time that a novel influenza strain is identified and the time that outbreaks begin to occur in the United States.

3. Outbreaks may occur simultaneously throughout much of the United States, preventing shifts in human and material resources that normally occur with other natural localized or regional disasters.

4. The effect of an influenza pandemic on individual communities should be relatively prolonged -- weeks to months.

5. The impact of the next pandemic could have a devastating effect on the health and well being of the American public. NJPH estimates that in New Jersey alone, during a 2 – 3 month period –

- Up to 4 million persons should be infected
- Up to 2 million persons should become clinically ill
- Up to 1 million persons should require outpatient care
- Up to 24,000 persons should be hospitalized
- Up to 6,000 persons should die

6. Effective preventive and therapeutic measures -- including vaccines and antiviral agents should likely be in short supply, as well as antibiotics to treat secondary infections.

7. Health-care workers and other first responders should likely be at even higher risk of exposure and illness than the general population, further impeding the care of victims.

8. Widespread illness in the community should also increase the likelihood of sudden and potentially significant shortages of personnel in other sectors who provide critical community services, including but not limited to, military personnel, police, firefighters, utility workers, and transportation workers.

3. Assumptions: Bioterrorism

1. It is very possible, and likely in a national or global sense, an act of bioterrorism is imminent in any given location.
2. The release of a biological agent should likely go unnoticed until infected persons present for medical treatment.
3. Most local public health and health care systems should be overwhelmed by community requests for information, prophylaxis and treatment when a bioterrorist threat or event becomes public knowledge.
4. Public health officials should need to work closely with law enforcement and other traditional first responders in a bioterrorism event.
5. Illnesses resulting from a bioterrorist release may be very difficult to differentiate from a naturally occurring outbreak of disease.

C. LOCAL IDEP LEADERSHIP

The protection of the health and welfare of the residents of New Jersey must be managed at the local level. Technical assistance, resources and materiel from the state may be provided when requested or in cases where emergency needs exceed the capability of local response resources. However, in a very large outbreak of disease, many communities should be affected and the state may not be able to meet all requests for assistance. With assistance from state agencies, **local jurisdictions are** responsible for:

1. Communication of information regarding prevention and control measures and local effects of disease.
2. Maintenance of public health and essential community functions during periods of high absenteeism.
3. Vaccine/pharmaceutical management and administration/dispensing.

D. PLAN DEVELOPMENT AND MAINTENANCE

1. Role of the Local Health Department in Infectious Disease Emergency Planning and Response

1. The local health department should assume a leadership role in local infectious disease emergency planning and response. It should:

- Establish provisions for public notification, comments, etc. These notification and alerting lists should be reviewed quarterly.
- Develop and maintain an IDEP in collaboration with other local agencies.
- Identify resources (personnel, supplies), both available and needed, to carry out an emergency immunization/medication dispensing clinic.
- Assist other departments and agencies with IDEP plan development.
- Coordinate IDEP exercises as needed.
- Conduct IDEP training as needed.

2. Other local departments and agencies with responsibilities under this plan should develop and maintain procedures for implementing an IDEP. These procedures should be reviewed at least annually and revised as needed.
3. The Commonwealth of New Jersey shall provide assistance to local health departments as provided for in the Commonwealth of New Jersey's Comprehensive Emergency Management Plan.

The local health department should work with the local emergency planning committee (LEPC) to develop the IDEP. The New Jersey's Department of Public Health (NJPH) and the New Jersey Emergency Management Agency (NJMA) should be available to lend technical assistance for plan development. Items that shall be reviewed annually for possible updating include, but are not limited to, the following:

1. Community and facility notification and alerting lists, including identity and phone numbers of appropriate personnel.
2. Lists of priority personnel for receipt of vaccine/pharmaceuticals.
3. Inventories of critical equipment, supplies, and other resources.

In addition, facility and community-specific functions and procedures should be reviewed and revised as appropriate.

E. UPDATE POLICY

The following policies apply to the review and updating of an IDEP.

1. It is the responsibility of the chief local health official to coordinate the review and update of an IDEP. The departments, agencies, communities, facilities, and others who have a role in infectious disease response under the plan should provide support. It is the responsibility of the mayor or the chief executive of each community to delegate responsibility for updating of community information.

2. The plan should be updated as necessary on an annual basis. The plan should be completed or reviewed within the past year.
3. Departments, agencies and facilities that maintain annexes and/or procedures that are a part of this plan should review that portion of the plan pertaining to their function on an annual basis.
4. The chief local health officer should facilitate and ensure the distribution of the updated plan to appropriate entities.

F. DIRECTIONS AND CONTROL

The purpose of direction and control is to provide for effective leadership, coordination and unified response during an infectious disease emergency. All communities have emergency preparedness plans sometimes known as the Comprehensive Emergency Management Plan (CEMP) -- to cope with major disasters such as hurricanes, plane crashes and hazardous materials events. These plans address many aspects of planning, including command and control functions, descriptions of emergency communication systems, hospital and medical care resources, and other key response elements that are relevant to infectious disease emergencies. However, infectious disease planning should require additional functions that are usually not included in the CEMP, such as delivery of vaccines and pharmaceuticals. One of the main differences between some infectious disease emergencies and other natural disasters is the widespread nature of health effects (along with disruption of critical human infrastructure because of those health effects), which require expansion of the typical disaster management team.

1. Essential Functions for Which Operational Procedures Should Be Developed

The local health department should oversee the development and implementation of operational procedures relevant to infectious diseases for the following essential functions:

- Communications
- Emergency Response
- Emergency Clinic Management and Operations

An infectious disease emergency should require a broad range of planning and response organizations including local government, public health, medical, emergency

response, social service, media and law enforcement. Public health and medical response organizations are typically trained to operate within their agency command structure. They are rarely called upon to perform their duties as part of a unified and integrated multi-organizational response, such as that required for an infectious disease emergency. Therefore, this plan calls for implementation of a strong system of direction and control.

2. Local Agencies and Staff that Should Participate in Infectious Disease Emergency Planning and Response

- Local hospitals or health centers
- Local public health
- Emergency medical services
- Local health care providers (including nursing organizations)
- Police department
- Fire department
- Animal inspectors
- Animal control officers (ACOs)
- Veterinarians
- Public information officer (or designee)
- School nurse(s)
- School administrator
- Representative(s) from the business community
- Representative(s) from civic and volunteer organizations
- Local media
- Social service organizations

G. RESPONSE PROCEDURES

The NJPH shall be the lead state agency for response to an infectious disease emergency. The NJPH should disseminate information regarding an infectious disease emergency to the local health department, including information on prevention and control. The NJPH also advises the New Jersey's Emergency Management Agency (NJEMA) about directing additional resources to local communities to assist in responding to infectious disease emergencies.

1. Local Unified Command

This plan addresses the need to ensure direction and control for a multi-jurisdiction/multi-agency response to an outbreak of disease. The concept of unified command means that all agencies that have jurisdictional responsibilities and authority at an incident should contribute to:

- Determining overall response objectives
- Selecting response strategies
- Ensuring joint planning and application of tactical activities
- Ensuring integrated planning and application of operational requirements including emergency measures and vaccine management/pharmaceutical distribution
- Maximizing use of available resources
- Ensuring dissemination of accurate and consistent information

2. Role of the Mayor or Chief Elected Official in Infectious Disease Emergency Planning and Response

The chief elected official of the community is responsible for the health and safety of the citizens of the community. Prior to an infectious disease emergency, the chief elected official should have appointed a local infectious disease coordinator and a public information officer. During an infectious disease emergency, the chief elected official should:

- Decide whether the local infectious disease coordinator or someone else should function as the incident commander during an infectious disease emergency.
- Assess the overall situation including the level of resources needed to deal with the problem.
- Determine who has resources and capacities to share in an infectious disease emergency and how these resources can be obtained.
- Consider the need for a local emergency declaration in consultation with the infectious disease coordinator and emergency manager.
- Be provided with copies of all press releases and summaries of all statements provided to the media in live or taped broadcasts.
- Set up regular situation updates with the infectious disease coordinator.
- Refer specific questions to the public information officer, but be prepared to answer policy related questions in coordination with the incident commander.

3. Responsibilities for Infectious Disease Emergency Planning and Response

The chief elected official should appoint a local infectious disease coordinator. The local infectious disease coordinator may be the director of health or another person. The local infectious disease coordinator is responsible for planning and managing an infectious disease emergency during the pre-emergency period, during an emerging alert, and during the emergency and post emergency periods.

H. COMMUNICATIONS

The purpose of communications is to ensure an efficient flow of accurate and consistent information during an infectious disease emergency, to facilitate communication among federal, state and local agencies about disease activity and to describe the system for providing information to the general public through the media and other information outlets. Dissemination and sharing of timely and accurate information among public health officials, government officials, medical care providers, the media and the general public should be one of the most important facets of the response.

1. Assumptions Upon Which the Communications Section of the IDEP is Based

1. Different types of information should have to be communicated, often to different audiences.
2. There should be widespread circulation of conflicting information, misinformation and rumors. Communication must be coordinated among all relevant agencies to ensure consistent messages to the general public.
3. There should be a great demand for accurate and timely information regarding:

- How many are ill, who is affected and where they are
- Basic disease information
- Disease complications and mortality
- Disease control efforts, including availability and use of vaccines, antivirals and other preventive and treatment measures
- “Do’s and Don’ts” for the general public
- Availability of essential community services

4. At the state level, it is possible that a priority list for receipt of vaccine/pharmaceuticals should be needed. Depending on existing supplies and supplies available through the Strategic National Stockpile (SNS), there should be a special need for information for the general public about availability of vaccine/pharmaceuticals. In the event of shortages, the targeted group may have to be further prioritized. Information should include the rationale for the list, how decisions were made, and what other control measures people can take until vaccine and or antibiotics are available for everyone.

5. Public education should be an important part of the immunization/pharmaceutical campaign because it is likely that the following problems should be encountered:

- Any symptom or illness that closely follows vaccination may be attributed to the vaccine and any febrile respiratory illness that occurs post-vaccination should be viewed as vaccine failure. (ED Kilbourne. National Immunization for Pandemic Influenza. Hospital Practice 1976:15-21)
- Prophylactic antibiotics/antivirals may need to be taken for a period of up to 60 days, or longer, and the recipient should need clear instructions on how to complete the course of treatment and where to get additional doses of antibiotics/antivirals.

6. Certain groups should be hard to reach, including people whose primary language is not English, people who are homeless, people who are hearing and visually impaired, etc...

7. Local resources, such as community-based organizations, mutual assistance or associations, and linguistically and culturally relevant media outlets should be identified prospectively.

8. During a prolonged infectious disease emergency such as influenza pandemic or a person to person transmitted BT event, demand for information by health care providers should be so great that traditional methods for educating health care providers should have to be expanded.

I. LOCAL COMMUNICATION RESPONSE PROCEDURES

1. Communication Responsibilities of the Local Health Department

- During an infectious disease emergency, local health department should have primary responsibility for:
- Meeting with the local infectious disease planning coordinator and public information officer to review the communication plan. The public information officer should monitor the situation and be prepared to respond to public and media requests for information.

- Setting up a **Local Joint Information Center** with the public information officer to provide and disseminate accurate information to the general public.
- Releasing information through the Local Joint Information Center concerning what volunteer goods and services are needed, and where volunteers and donors may go to deliver such goods or potential services.
- Gathering all records kept during all phases of the incident and preparing a chronological summary of events, actions taken, inquiries made, and response given.
- Collecting newspaper clippings and TV videotapes, if available.
- Surveying the local emergency planning committee and the local media for suggestions to improve emergency response procedures for future emergencies.

2. Role of the Local Public Information Officer

All news releases should be handled by the authorized public information officer.

During an infectious disease emergency, the public information officer should have primary responsibility for:

- Ensuring that all information is clear, confirmed, and approved by appropriate authority before release to the media or public.
- Not releasing unconfirmed information or speculating on the extent of the emergency, despite repeated urging by reporters to do so.
- Monitoring news programs and reviewing news articles for accuracy and correcting serious misinformation whenever possible.
- Establishing a Joint Information Center/Media Center and providing sufficient staffing and telephones to handle incoming media and public inquiries and gathering information.
- Providing public information according to priorities.
- Ensuring that official spokespersons are thoroughly briefed about all aspects of the emergency.
- Keeping the infectious disease planning coordinator informed of all media actions taken or planned.
- Keeping public information officers in other jurisdictions and at other government levels informed of information released.
- Maintaining a log and file of all information.
- Releasing emergency instructions/information to the public as necessary. (Closing of public facilities, where to get vaccine, etc.).
- Releasing prevention, control and treatment information, as appropriate.

- Responding promptly to media and public calls.
- Releasing public inquiry ("rumor control") telephone line number when it is staffed.
- Attending periodic briefings and planning sessions.
- Considering additional methods of distributing emergency instructions.
- Arranging media briefings/press conferences on a regular or "as needed" basis.
- Preparing news releases, as required.
- Providing emergency information in foreign languages, as required.
- Releasing morbidity and mortality figures when obtained.

3. Communicating with Special Needs Populations/Groups

As part of infectious disease planning, local health departments should identify groups in their communities that should require special efforts to ensure they receive all information necessary to protect them during an infectious disease emergency. Outreach conducted during the pre-emergency period should ensure that channels are in place to facilitate communication during a real emergency. Special needs populations include but are not limited to: native people (Native Americans, Hawaiians and Pacific Islanders), elderly, children, culturally and/or linguistically distinct communities, deaf and hard of hearing, blind and visually impaired, people with disabilities, people that are homebound, people that are institutionalized, recent immigrants, migrant/seasonal farm-workers, people living with HIV/AIDS (or other immuno-deficient disease), people living with mental illnesses, the homeless and others.

J. EMERGENCY RESPONSE

1. Assumptions Upon Which the Emergency Response Section of the IDEP is Based

Infectious disease emergencies can be broadly grouped into two categories:

a. Non-Communicable Infectious Disease Emergencies

The response to non-communicable infectious disease and other biologic emergencies is similar to typical local disasters with little or no advance notice. Examples of non-communicable events include Bio-Terrorism attacks with anthrax or widespread food-borne toxicities, like paralytic shellfish poisoning mediated through a seafood

processing plant. Individuals exposed in a non-communicable event should require medical triage and evaluation. However; the spread of the event should be limited because of the lack of person to person transmission. Chaos and misinformation should be significant problems to contend with. There may be a need for widespread vaccination and medication dispensing clinics.

b. Communicable Infectious Disease Emergencies

Communicable infectious disease emergencies, such as an influenza pandemic or a smallpox outbreak, should be widespread, with many geographic areas possibly affected -simultaneously. Thus, each community should have to be prepared to act on its own, rather than pooling resources from several contiguous jurisdictions, or relying on state personnel for help. Chaos and misinformation should be significant problems to contend with. There may be a need for widespread vaccination and medication dispensing clinics.

If illness associated with an infectious disease emergency is especially severe, health services could easily become overwhelmed very quickly with the following:

- Shortfalls of ICU beds, ventilators and other critical-care needs
- Shortages of antibiotics and/or antiviral agents
- Needs for ancillary or "non-traditional" treatment centers
- High demand for mortuary/funeral services
- High demand for social and counseling services

Unlike natural disasters, demands on medical care in each community might be prolonged if the illness spreads from person to person.

Unlike the typical disaster, essential community service personnel themselves (e.g., medical-care personnel, police, firefighters, ambulance drivers and other first responders) should be just as likely or even more likely (because of increased exposure) to be affected by a communicable infectious disease emergency than the general public.

Because of the threat of exposure to influenza or other infectious diseases, the elderly and other high-risk and special-needs populations may be fearful of leaving their homes to seek medical attention for chronic medical conditions, and may require home visits for basic needs and health care.

In summary, high attack rates of a communicable disease or the perception of personal danger should place overwhelming demands on the health care system. Health care providers, emergency response and public safety personnel should be equally or more likely to become infected than the general public. Certain high-risk groups should be less likely to have access to information and services (e.g., people who are homeless, homebound, poor, undocumented or who do not speak English). Because the epidemic can be widespread, it is unlikely that resources could be diverted from other geographic areas. Every community should have to be prepared to be self-sufficient, while at the same time sharing resources such as hospitals, mortuary services, etc.

K. RESPONSE PROCEDURES

In order to contain the spread of a contagious illness, public health authorities rely on many strategies. Two of these strategies are isolation and quarantine. Both are common practices in public health and both aim to control exposure to infected or potentially infected individuals. Both may be undertaken voluntarily or compelled by public health authorities. The two strategies differ in that isolation applies to people who are known to have an illness and quarantine applies to those who have been exposed to an illness but who may or may not become infected.

1. Isolation: For People Who are Ill

Isolation of people who have a specific illness separates them from healthy people and restricts their movement to stop the spread of that illness. Isolation allows for focused delivery of specialized health care to people who are ill, and it protects healthy people from getting sick. People in isolation may be cared for in their homes, in hospitals, or at designated health care facilities. Isolation is a standard procedure used in hospitals today for patients with tuberculosis (TB) and other infectious diseases. In most cases, isolation is voluntary; however, many levels of government (federal, state, and local) have basic authority to compel isolation of sick people to protect the public.

2. Quarantine: For People Who Have Been Exposed but are Not Ill

Quarantine, in contrast, applies to people who have been exposed and may be infected but are not yet ill. Separating exposed people and restricting their movements is intended to stop the spread of that illness.

3. Contingency Plans to Meet the Needs of Persons Confined to Their Homes

During an extended or widespread emergency, persons may be confined to their homes by choice, out of fear of being exposed and becoming ill, or by direction from state or local health officials in order to reduce transmission in the community.

The provision of food, medical and other essential support for persons confined to their homes should be the responsibility of local communities. Local communities are encouraged to make use of civic organizations and other volunteers to meet these needs. For instance, local agencies already engaged in providing services to the homebound (Meals-on-Wheels, etc.) may become the nucleus for voluntary efforts to provide services to people confined to their homes. In addition, there should likely be situations in which care providers of children, people with special needs or the elderly should become ill and unable to care for their dependents. Communities should need to have plans in place to identify these situations (e.g., hotlines and or home visiting programs) and contingency plans to care for these individuals. Resources to staff hotlines or home visiting programs include civic/volunteer organizations, local colleges and senior citizens. Using these resources on a regular basis to staff flu clinics, health fairs, etc. should ensure a ready group of volunteers in an infectious disease emergency.

4. Medical Care for People Sick at Home

Families should need information about how to take care of sick family members at home, and guidelines regarding when to seek professional medical care. This first-line triage should be essential to eliminating unnecessary calls and decreasing the burden on health care providers, freeing them to care for the seriously ill.

5. Maintenance of Other Essential Community Services

Personnel, who provide essential community services, including public safety and emergency response, should be as likely to become ill during an infectious disease emergency as the general public. Contingency plans for back up for essential personnel

during periods of high absenteeism need to be in place to ensure continuation of essential community services during the pandemic. Each local agency should review and update (or develop) lists of essential services and personnel. Contingency plans should be developed to provide backup for any personnel whose absence would pose a threat to public safety or would significantly interfere with the on-going response to the pandemic. Backup personnel could come from reassignment of personnel from non-essential programs within local agencies, retired personnel and/or private-sector personnel with relevant expertise (After: California Department of Health and Human Services Response Plan).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. BIOTERRORISM SURVEILLANCE AND EPIDEMIOLOGIC RESPONSE PLAN

The New Jersey Department of Health and Senior Services (NJDHSS) has also requested NPS to provide them with a Bioterrorism Surveillance and Epidemiologic Response Plan that should be the product of collaborative efforts involving public health partners at the local, state, and federal levels. This response plan again is based on the California's Health and Human Services Response plan.

A. INTRODUCTION AND BACKGROUND

Bioterrorism and its potential for mass destruction have been subjects of increasing concern. Terrorist groups have used or threatened to use biological agents in a variety of circumstances, both domestically and internationally. Current concerns regarding the threat of bioterrorism result from the production of biological weapons for use in the 1991 Gulf War and from the increasing number of countries that are engaged in the proliferation of such weapons. As many as ten countries possess offensive biological weapons programs and the existence of these programs increases the likelihood that biological expertise should be transferred, directly or indirectly, to groups and individuals with grievances against the government or society.

The growth of religious cults and extremist political groups also increases the threat of bioterrorism - today. New Jersey is vulnerable to bioterrorist incidents. New Jersey consists of a population of 8,698,879 and is a large economy that continues to be a major port of entry for travelers to the U.S. The public health infrastructure at the local and state levels must be prepared to detect, control, and prevent illness and injury resulting from biological and chemical terrorism, especially a covert terrorist attack. Preparation for bioterrorism involves strengthening of the existing infrastructure for the surveillance of infectious diseases; detection, and investigation of outbreaks; identification of etiologic agents and their modes of transmission; the development of prevention and control strategies; and; the mobilization and management of resources required to respond to disease outbreaks and other health emergencies.

The following section of this plan addresses surveillance and epidemiologic response. The overall NJDHSS plan should include sections on bioterrorism preparedness; surveillance and epidemiologic response; the laboratory's role in bioterrorism detection and response; health and medical response; and, communication. The plan should be compliant with the Standardized Emergency Management System for the request and activation of resources. This plan is a working document that should be updated to reflect new developments and lessons learned in bioterrorism preparedness and response.

B. SURVEILLANCE AND EPIDEMIOLOGIC RESPONSE SECTION

Early detection of bioterrorist events is essential because; although, most diseases caused by bioterrorist threat agents are rapidly fatal, many are readily treatable and/or preventable with timely administration of appropriate antibiotics, antiserum, vaccination, and/or prophylaxis following exposure. If the bioterrorist event involves a disease that is transmissible from person-to-person, early detection would also allow timely implementation of isolation and/or quarantine guidelines to prevent additional cases.

A coordinated epidemiologic investigation must be conducted as soon as a suspected bioterrorist event is detected to determine the etiology and source of the outbreak and to identify the most effective interventions to save as many lives as possible. The objectives of this bioterrorism surveillance and epidemiologic response section are:

1. To describe how NJDHSS plans to enhance surveillance and epidemiologic response for suspected bioterrorist event(s);
2. To define roles and relationships between local health departments and NJDHSS partners in bioterrorist surveillance and epidemiologic response activities; and
3. To provide guidance to local health departments regarding bioterrorism surveillance and response strategies at the local level.

C. BIOTERRORIST EVENT DEFINITIONS

For the earliest recognition of bioterrorism, public health personnel who conduct traditional disease investigations must become familiar with unusual disease events that

should increase the index of suspicion for bioterrorism. To help facilitate this early recognition among local public health officials, this section of the bioterrorism surveillance and epidemiology document attempts to define disease scenarios that may represent the initial report of a bioterrorist event.

The bioterrorist threat agents deemed the highest priority by the Centers for Disease Control and Prevention (CDC) are the causes of: anthrax (*Bacillus anthracis)*, botulism (*Clostridium botulinum),* plague *(Yersinia pestis),* smallpox (variola major)*,* tularemia *(Francisella tularensis),* and viral hemorrhagic fevers (filoviruses and arena viruses).

These agents are prioritized by the CDC based on their potential ease of dissemination, ability to cause high mortality, the need for special preparations such as vaccine development or antibiotic stockpiles and finally, the social disruption they could cause. With the exceptions of smallpox (the endemic transmission of which has been globally eradicated) and filoviruses, human diseases caused by these threat agents do occur in New Jersey, albeit rarely. NJDHSS' Division of Communicable Disease Control (DCDC) staff is available 24 hours a day to assist local health departments in determining whether an unusual illness or cluster of illnesses should be considered suspicious for bioterrorism.

1. Highly Suggestive of Bioterrorism

A single definitively diagnosed or strongly suspected case of:

- Smallpox
- Inhalational anthrax
- Coetaneous anthrax (with no known risk factors compatible with naturally-occurring disease)
- Viral hemorrhagic fever (in a patient with no international travel history)

OR

- Greater than one case of:
- Pneumonic plague
- Pneumonic tularemia with at least one laboratory confirmed case, no known compatible risk factors, and occurring in a brief time period

OR

- A higher than expected number of unexplained deaths occurring in a brief time period within a defined geographic region.

2. Moderately Suggestive of Bioterrorism

A single definitively diagnosed or strongly suspected case of:

- Pneumonic plague
- Pneumonic tularemia occurring in a patient with no known compatible risk factors

OR

- A cluster of brucellosis cases occurring in persons with no known compatible risk factors

OR

- A higher than expected number of presumptively diagnosed botulism cases with no known compatible risk factors occurring in a brief time period

OR

- A higher than expected number of cases of unexplained severe respiratory illness requiring hospitalization, especially if occurring outside the usual flu transmission season

OR

- The occurrence of any unusual epidemiologic features in a seemingly natural outbreak
- (e.g., the absence of the usual risk factors for disease, or the presence of unusual risk factors, or greater than expected morbidity or mortality).
-

D. CONFIRMATION

Confirmation that a bioterrorism event definition has been met may require consultation among local, state, and/or federal public health officials. NJDHSS disease experts, including laboratorians, stand ready to assist local public health officials in assessing the clinical, laboratory, and epidemiologic features of a disease event, to determine whether the disease scenario is suspicious for bioterrorism. The disease-specific investigation algorithms may be useful in helping to determine whether bioterrorism should be suspected

E. NOTIFICATION OF SUSPECTED/CONFIRMED BIOTERRORIST EVENTS

Once local, state and/or federal public health officials confirm that a disease scenario meets the event definition for bioterrorism, local, state, and federal bioterrorism response partners should be notified immediately. At the local level, the health department (LHD) is responsible for contacting their local Federal Bureau of Investigation (FBI) office. FBI is the lead law enforcement agency for crisis management of a bioterrorist event. The State should be notified by the LHD through two major notification routes. The LHD should contact the Governor's Office of Emergency Services (OES) and should notify the New Jersey Department of Health and Senior Services (NJDHSS) directly by contacting the Division of Communicable Disease Control's Duty Officer of the Day (DCDC DOD) or a DCDC Bioterrorism Key Contact. The DCDC DOD (assumption) is on-call 24 hours a day and is responsible for responding to all calls involving infectious disease emergencies. When the LHD contacts the state through the OES, the LHD should call the OES Warning Control Center. The OES Warning Control Center receives warnings and notifications of all disasters in New Jersey, including acts of bioterrorism, and is responsible for notifying all appropriate local, state, and federal agencies. In the event of bioterrorism, the OES should notify NJDHSS Duty Officer (NJDHSS DO). The NJDHSS DO triages calls regarding public health emergencies. The NJDHSS DO receiving a call involving a suspected bioterrorist event should notify the NJDHSS Emergency Preparedness Office (NJDHSS EPO) Counterterrorism Coordinator and the DCDC DOD or a DCDC Bioterrorism Key Contact.

Within DCDC, four Bioterrorism Key Contacts have been identified: the State Epidemiologist, the Bioterrorism Surveillance and Epidemiologic Response Team (BSERT) Leader, the Viral and Rickettsial Disease Laboratory (VRDL) Chief, and the Microbial Diseases Laboratory (MDL) Chief. Only one Key Contact is required to be contacted, but they should be called IN SEQUENCAL ORDER until one is successfully reached (i.e., if the State Epidemiologist cannot be contacted, the BSERT Leader should be called next).

When the LHD calls the DCDC directly, they may call either the DCDC DOD or a DCDC Bioterrorism Key Contact. If the DCDC DOD is the first to be notified by the LHD, the DCDC DOD should call the NJDHSS DO. The DCDC DOD should also call the four DCDC Bioterrorism Key Contacts IN SEQUENCAL ORDER until one is reached.

The first DCDC Bioterrorism Key Contact to be reached is responsible for ensuring the notification of all members of the DCDC Bioterrorism Working Group: DCDC Chief, Disease Investigations and Surveillance Branch (DISB) Chief, Disease Investigations Section (DIS) Chief, Veterinary Public Health Section (VPHS) Chief, Vector Borne Diseases Section (VBDS) Chief, Surveillance and Statistics Section (SSS) Chief, BSERT Leader, VRDL Chief, and MDL Chief. If a member of the Working Group cannot be contacted, his or her designated alternate should be contacted. If the DCDC Bioterrorism Key Contact is the first to be notified by the LHD, the DCDC Bioterrorism Key Contact should also notify the DCDC DOD and the NJDHSS DO. The Key Contact is also responsible for verifying that the local FBI office has already been contacted and, if not, to notify it of the situation.

When the NJDHSS DO first learns of a bioterrorist event through DCDC (either the DCDC DOD or a DCDC Bioterrorism Key Contact), he or she should notify the OES Warning Control Center and the NJDHSS EPO Counterterrorism Coordinator. The EPO Counterterrorism Coordinator should call the DCDC DOD or the DCDC Bioterrorism Key Contact to coordinate communications with the DCDC Bioterrorism Working Group.

Once the DCDC Bioterrorism Working Group is notified, the Working Group should contact the Health Officers of the appropriate LHDs. The Health Officers are then responsible for the notification of the appropriate personnel in their jurisdictions. The Working Group should also notify the Bioterrorism Preparedness and Response Program (BPRP) at the Centers for Disease Control and Prevention (CDC).

1. Notification

As previously mentioned we are following the California's Emergency Response, as such the figure below also be used by the New Jersey Hospital

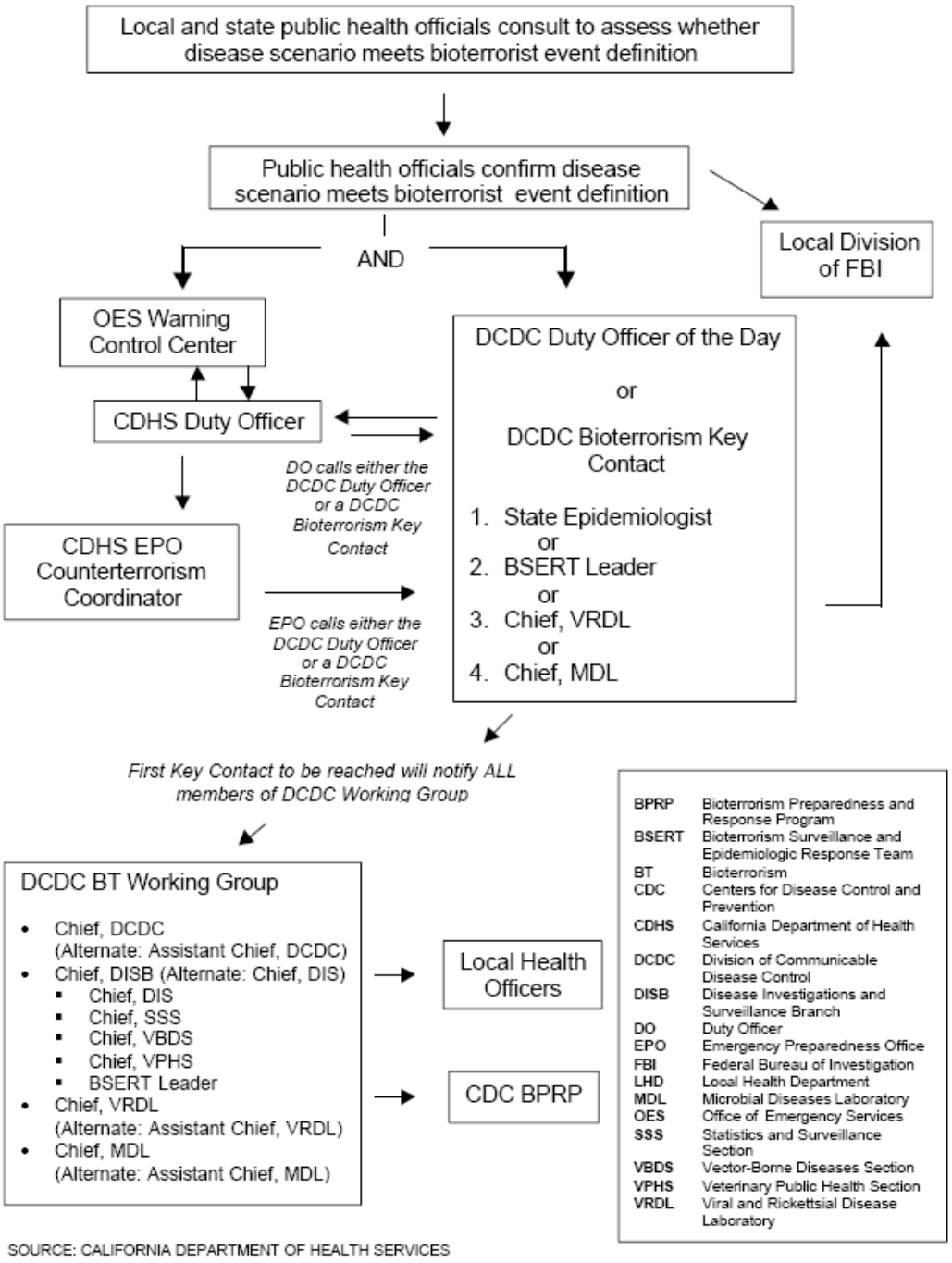


Figure 31. Contact Chart (From: California DHS)

F. SURVEILLANCE SYSTEMS FOR DETECTING BIOTERRORIST EVENTS

1. Introduction

a. Essential Role of Surveillance

An act of terrorism involving the release of a biological agent is a major public health emergency and requires immediate response. In contrast to other emergency events, an attack with a biological agent should probably not be detected at the time the event occurs, nor should it elicit an immediate response from police, fire or emergency medical services personnel. This is because an attack with a biological agent is likely to be covert and also because there is a delay between exposure and the onset of symptoms (incubation period) which can be as long as several days, weeks or even months.

The difficulty of early detection is further compounded because diseases caused by many of the likely bioterrorist agents may not be accurately diagnosed until late in their course, since early symptoms tend to be nonspecific. Finally, most clinicians in the United States have little or no experience with these agents (e.g., inhalational anthrax or smallpox).

Early detection of bioterrorist events is essential because although most bioterrorist threat diseases[1] are rapidly fatal and some are easily transmitted from person-to-person, many bioterrorist threat diseases are readily treatable and/or preventable if patients are provided timely and proper antibiotics, antiserum and/or immunization following exposure. Conversely, bioterrorist threat diseases may prove fatal if therapy or prophylaxis is delayed until classic symptoms develop. Early detection and rapid investigation by public health epidemiologists is critical for determining the scope and magnitude of the exposure. Delays in detection and/or epidemiologic investigation may result in illness and deaths.

b. Roles and Responsibilities of NJDHSS

The roles and responsibilities of NJDHSS in bioterrorism surveillance include:

1. Supporting local health departments to increase awareness of clinicians and laboratorians about bioterrorist threat agents and diseases
2. Strengthening existing disease surveillance systems

3. Utilizing and/or developing additional surveillance systems which might be useful in detecting illness resulting from bioterrorist threat agents

4. Providing technical assistance to local health jurisdictions implementing pilot surveillance systems for detecting bioterrorist events

5. Coordinating expanded surveillance in the affected jurisdictions[1] in the event of a suspected bioterrorist event or other biologic disaster. Specific NJDHSS activities to enhance bioterrorism surveillance include:

- The revision of state disease reporting regulations to make all suspected and confirmed cases of bioterrorist threat diseases immediately reportable.
- The implementation of a rapid electronic laboratory disease reporting and alert system.
- The development of tools for increasing awareness about bioterrorism (e.g., slide sets, fact sheets, training curricula).
- The implementation of informal intra- and inter-departmental notification of unusual health events detected by existing surveillance systems (e.g., veterinary surveillance, botulinum antitoxin requests, influenza surveillance project).
- The provision of technical assistance to local health departments piloting systems or mechanisms that could be useful in the detection of bioterrorist events including surrogate measure monitoring (e.g., hospital admission diagnoses; 911 calls) and clinical syndrome reporting.

c. Roles and Responsibilities of Local Health Departments

The local health department has the lead role in the early detection and identification of a bioterrorist event. And, in the event of a confirmed bioterrorist event or other large biologic disaster, the local health department should be responsible for initiating expanded surveillance. At a minimum, local health departments should implement activities to educate clinicians and laboratorians about:

- Their disease reporting responsibilities, especially of outbreaks and unusual disease occurrences.
- Bioterrorist threat agents and diseases, and
- How to contact the local health department in case of a public health emergency.

1 The bioterrorist threat agents deemed the highest priority by the Centers for Disease Control and Prevention (CDC) are the causes of: anthrax (Bacillus anthracis), botulism (Clostridium botulinum), plague (Yersinia pestis), smallpox (variola major), tularemia (Francisella tularensis), and viral hemorrhagic fevers (filoviruses and arena viruses). (See Appendix A for complete list of CDC high-priority diseases).

Local health departments could also establish and/or strengthen informal disease reporting links with other partners (e.g., animal control, veterinarians, medical examiners and coroners, infection control practitioners, poison control centers, quarantine personnel).

If resources are available, local health departments may opt to implement pilot surveillance projects for improving the early detection of bioterrorist threat diseases and infectious disease outbreaks. The following section of the NJDHSS bioterrorism surveillance and epidemiology plan includes an overview of activities which the state plans to implement to improve surveillance for bioterrorist events and a description of additional activities, which could be considered at the state or local health department level if resources are available.

2. Overview of Strategies for Improving Bioterrorism Surveillance

Existing disease reporting systems in California are neither sensitive nor timely enough to allow a rapid response to a bioterrorist event. Current estimates are that only about 20% of some reportable diseases are actually reported in some NJ counties[2]. Physicians are not fully meeting their legally mandated requirements to report communicable disease occurrences because of lack of knowledge, time, interest, and the current cumbersome (paper-based) reporting process. Early detection of bioterrorist events may be achieved through a spectrum of activities. At one end of the spectrum are detection systems that are more specific but less timely, which include mandatory reporting of diseases and conditions by health care professionals and laboratories. At the opposite end of the spectrum are detection systems that are more sensitive and timely, but less specific. For example, emergency medical services systems could collect sensitive and timely data on hospital diversion hours or 911 calls, but follow-up investigation is needed to determine whether an increase in diversions or calls is due to an unusual health event. Strategies for strengthening the early detection of bioterrorist events may be grouped into the following categories:

- Increasing awareness of clinicians and laboratorians
- Strengthening the communicable disease reporting system

2 System Requirements and Feasibility Analysis for Communicable Disease Reporting via the Internet in California, Lawrence Livermore National Laboratory report sponsored by CDHS (October 1998).

- Utilizing additional surveillance systems
- Piloting novel detection systems

3. Increasing Awareness of Clinicians and Laboratorians

Early detection depends upon healthcare provider and laboratorian recognition and reporting of suspicious illnesses and organisms. Increasing the awareness of clinicians and laboratorians about bioterrorist threat agents and diseases is an important strategy for improving bioterrorism surveillance. Some strategies and tools that NJDHSS and local health departments could use to increase awareness about bioterrorism are listed below.

a. Strategies for Increasing Awareness about Bioterrorism

Education of clinicians and laboratorians about their essential roles in recognizing and reporting a possible bioterrorist event and/or other infectious disease outbreak(s) could be achieved in a variety of settings. Presentations could be given at clinical rounds at local hospitals and at meetings of local professional organizations, targeting specialists in internal medicine, emergency medicine, pediatrics, family practice, infectious diseases, critical care, pulmonary medicine, and pathology. Other target audiences include pre-hospital care providers, infection control practitioners, physician-trainees and medical students, medical examiners, veterinarians, and microbiologists. Training seminars are being given to public health laboratory personnel, health maintenance organization (HMO) laboratory personnel and other hospital laboratory personnel throughout New Jersey.

Bulletins on bioterrorism and fact sheets on the bioterrorist threat agents could be widely distributed to the medical and laboratory communities via the internet and via traditional means (mailing). Posters that list the notifiable diseases and remind health providers (emergency departments, intensive care, etc.) of their reporting obligations could also be printed and distributed. All of these activities provide an excellent opportunity for reinforcing surveillance and reporting in general.

b. Tools for Increasing Awareness about Bioterrorism

Training curricula, disease fact sheets, and other tools for increasing awareness about bioterrorism are being developed for distribution to local health

departments for use at the local level. Additional training materials are being developed for public health professionals and laboratorians including laboratory bench training and distance learning modules.

G. STRENGTHENING THE COMMUNICABLE DISEASE REPORTING SYSTEM

Approaches to strengthening the existing disease reporting system include:

1) Revision of disease reporting regulations to make all suspected and confirmed cases of bioterrorist threat diseases immediately reportable by health care providers and laboratories
2) Implementation of a rapid electronic laboratory disease alert and reporting system.

1. Reporting Regulations

Immediate reporting of all bioterrorist threat diseases is critical for limiting the impact of the bioterrorist event. Emergency amendments[3] to the New Jersey Code of Regulations (Title 17), effective as of November 5, 2001, made those diseases that pose a significant threat as agents of biological terrorism immediately reportable by health care providers[4] to the local health department (LHD); by the LHD to the NJDHSS; and by clinical laboratories, public health laboratories, and veterinary laboratories to the LHD.

The current status of the emergency regulations require health care providers to immediately report by telephone all suspected and confirmed cases of bioterrorist threat diseases, which include anthrax, botulism, brucellosis, plague (animal or human), smallpox (variola), tularemia, varicella (deaths only), viral hemorrhagic fevers, unusual diseases[5], and outbreaks of any disease to the local health department. In addition, the emergency regulations also require local health officers to immediately report to NJDHSS by telephone upon being notified of suspected or confirmed cases of the bioterrorist threat diseases listed above.

---

3 The emergency amendments to the New Jersey Code of Regulations (Title 17) are available on the Internet at http://www.dhs.nj.gov/regulation.

4 Health care providers include physicians, surgeons, veterinarians, podiatrists, physician assistants, registered nurses, nurse midwives, school nurses, infection control practitioners, medical examiners, coroners and dentists.

5 'Unusual disease' means a rare disease or a newly apparent or emerging disease or syndrome of uncertain etiology that a health care provider has reason to believe could possibly be caused by a transmissible infectious agent or by a microbial toxin

The emergency regulation amendments also expand reporting responsibilities of clinical laboratories, approved public health laboratories, and veterinary laboratories. In addition to the 18 communicable diseases that were already reportable to the local health department within 24 hours of providing results to the physician, the newly adopted emergency regulations require laboratories to report laboratory findings indicative of the specified bioterrorist threat agent to the local health department within one hour of providing results to the physician.

2. Electronic Laboratory Reporting

Monitoring electronic reports of requests for laboratory tests and laboratory test results could provide the earliest recognition of a bioterrorist incident.

H. UTILIZING ADDITIONAL SURVEILLANCE SYSTEMS FOR DETECTING ILLNESS RESULTING FROM BIOTERRORIST THREAT AGENTS

The integration of information from other surveillance systems into the routine communicable disease reporting system could facilitate the early detection of a bioterrorist event. Existing surveillance systems that are currently being integrated to facilitate bioterrorism surveillance are described in Section A of Appendix F and include veterinary surveillance, botulism surveillance, and influenza surveillance Project.

I. PILOTING NOVEL DETECTION METHODS SUCH AS SURROGATE MEASURE MONITORING AND CLINICAL SYNDROME REPORTING

Where resources are available, local health departments are developing systems for detecting and responding to non-specific increases in surrogate markers (e.g., absenteeism, emergency department presenting complaints, emergency department diversions) and increases in numbers of patients seeking care for specific clinical syndromes. NJDHSS should endeavor to provide technical assistance when requested and should monitor the progress of pilot projects.

1. Surrogate Indicator Monitoring

Indirect or surrogate indicators may be useful for monitoring the presence of abnormal levels of disease, as well as for detecting a bioterrorist event. Systems for monitoring surrogate indicator data should require the development of algorithms and

statistical methods for detecting unusual or suspicious events. Although surrogate measure data have the potential of being timely and sensitive, they are not specific. Unusual findings necessitate follow-up by the local public health department requiring significant resources.

Potential data sources include:

- 911 dispatch
- Emergency department diversions
- Emergency department visits or diagnoses
- Nurse advice call centers
- Poison control centers
- Over-the-counter pharmacy sales
- Medical examiner/vital statistics
- Hospital admissions/diagnoses
- Critical care unit admissions/diagnoses
- Absenteeism in schools/large worksites

2. Clinical Syndrome Reporting

Clinical syndrome surveillance, the reporting of clinical syndromes rather than specific diagnoses and/or laboratory-confirmed cases, has the potential for facilitating the early detection of a bioterrorist event. Clinical syndrome surveillance can be extremely resource-intensive since it requires the establishment of new infrastructure for collecting, reporting, and responding to data.

J. EPIDEMIOLOGIC RESPONSE TO SUSPECTED/CONFIRMED BIOTERRORIST EVENTS

Although the steps in the epidemiologic response to a suspected bioterrorist event should be similar to other communicable disease outbreaks, the tempo should be much faster. These steps are listed below in order; however, many should be conducted simultaneously, and the importance of a particular step may vary depending on the circumstances of the outbreak.

1. Confirmation

The first step in the epidemiologic response to a disease scenario suspicious for bioterrorism should be to reach a consensus that bioterrorism is moderately or strongly suspected, whether for a single case or for a cluster of cases (See Event Definitions, Section II). Local, state, and federal disease experts should help determine whether the clinical and/or laboratory findings are consistent with a bioterrorist threat agent and/or whether the epidemiologic evidence supports the suspicion of bioterrorism.

The NJDHSS Microbial Diseases Laboratory (MDL) or the Viral and Rickettsial Disease Laboratory (VRDL) should be involved in confirming the causative agent in a potential bioterrorist event (See Laboratory Section of the Bioterrorism Preparedness and Response Plan). However, in the case of diseases for which prompt laboratory diagnosis is not possible (e.g., smallpox), specimens should be forwarded to a national reference laboratory for laboratory confirmation, and clinical and other criteria should necessarily be relied upon to determine whether a disease scenario meets the event definition for bioterrorism.

2. Notification

Once it is agreed that the disease scenario meets the event definition for bioterrorism, local, state, and federal bioterrorism response partners should be immediately notified. The NJDHSS Bioterrorism Surveillance and Epidemiologic Response Team (BSERT) should be activated and should serve as the state's core epidemiologic rapid response team.

3. Coordination

New Jersey's epidemiologic response to a bioterrorist event should be coordinated by the NJDHSS/DCDC in the event of a multi-jurisdictional infectious disease outbreak. Local, state, and federal public health leaders should participate in the epidemiologic investigation under a joint command structure and the lead for the investigation should be determined through the joint command. In the event of a bioterrorist outbreak involving a single health jurisdiction, the NJDHSS/DCDC should be available to provide epidemiologic support if requested.

Several types of personnel may be required for the epidemiologic investigation including: interviewers, environmental health inspectors, disease control investigators,

*e*pidemiologists, data entry staff, and data managers. Personnel should be drawn from affected and from unaffected local health departments and from NJDHSS/DCDC. Finally, federal epidemiologic assistance can be requested from the Centers for Disease Control and Prevention (CDC). The epidemiologic investigation should be coordinated with the criminal investigation conducted by the Federal Bureau of Investigation (FBI), the lead agency in the crisis management of a bioterrorist event.

4. Communication

Information from the outbreak investigation should be communicated to other New Jersey bioterrorism response partners such as the Office of Emergency Services (OES) and the Emergency Medical Services Authority (EMSA) to help guide planning for distribution of medical resources, and to the FBI. In the event of an outbreak involving multiple health jurisdictions, release of public information regarding the epidemiologic investigation and response should be coordinated by the local health department public health information officers and the NJDHSS Office of Public Affairs (OPA) with the FBI to assure accurate and consistent public health messages (see Medical Response and Media Sections of the Bioterrorism Preparedness and Response Plan).

Messages may include information about the disease and its prevention, treatment and control, and the progress of the outbreak investigation. If the disease is thought to be transmissible from person-to-person, requests for locating contacts could be communicated through the media. Recommendations for treatment of cases and contacts should also be communicated directly to medical care providers by those coordinating the medical response (see Medical Response Section of the Bioterrorism Preparedness and Response Plan). Treatment and prophylaxis guidelines, infection control guidelines, and disease fact sheets should be included in the Medical Response Section of the Bioterrorism Plan.

5. Epidemiologic Investigation

In a multi-jurisdictional bioterrorist event, local, state, and federal public health leaders should participate in the epidemiologic investigation under a joint command structure. The lead for the epidemiologic investigation should be determined through the

joint command. In the event of a bioterrorist outbreak involving a single health jurisdiction, the NJDHSS/DCDC should be available to provide epidemiologic support if requested.

K. HYPOTHESIS-GENERATING INTERVIEWS

Hypothesis-generating interviews with the initial cases should be conducted as early as possible in the epidemiologic investigation to help identify the causal agent and possible modes and locations of exposure. If the specific etiologic agent for the illness has not been identified, investigators should need to ask a broad array of exploratory clinical and exposure questions to better characterize the disease outbreak. However, if the causal agent (or agents) has been identified, questionnaires with disease-specific clinical questions combined with exploratory exposure questions should be more appropriate. Template syndromic and disease-specific questionnaires have been developed for this purpose. Exploratory and in-depth risk exposure questions have been developed to assess various potential modes of exposure and have been included in both the syndromic and disease-specific questionnaires.

Regardless of whether the syndromic or the disease-specific questionnaires are used in hypothesis-generating interviews, the template questionnaires should have to be modified at the time of the event to reflect or incorporate available information and hypotheses. Information from the initial cases should be used to construct an epidemiologic curve, demographic and clinical profiles, and to determine possible sources of exposure.

1. Case Definition

Using the data from the initial hypothesis-generating interviews, a working case definition should be established. A uniform case definition should be used to identify additional cases requiring follow-up and to provide a meaningful case count across jurisdictions.

2. Case Finding

Case finding should be conducted by local and state public health officials through alerts to multiple potential reporting sources, including:

- Public health officials and personnel
- Public health and clinical laboratories
- Hospitals, physicians, and infection control practitioners
- Emergency medical services
- Media

Public health alerts could recommend that persons with symptoms promptly seek health care. If the source of initial exposure is known, the alerts could also recommend that persons who believe that they have been exposed should telephone the local health department for further instructions.

Hotlines could be established at the local health department to receive calls from clinicians and the public about potential cases and contacts.

3. Case Interviews

Cases should be interviewed using a uniform questionnaire. A pre-prepared template questionnaire using information generated from the hypothesis-generating interviews, to further characterize the mode or source of the exposure.

In a multi-jurisdictional event, interviews should be conducted by local and state public health personnel.

4. Data Analysis

Data entry and analysis for epidemiologic investigation and contact tracing activities should be coordinated by NJDHSS/DCDC when a bioterrorist event involves multiple health jurisdictions. If a bioterrorist event involves a single health jurisdiction, the NJDHSS/DCDC should be available to provide data analysis support to the local health department. The primary objective of data analysis should be to provide timely, comprehensive data for public health and public safety decision-makers to formulate control measures to mitigate the public health impact of the event. The outbreak investigation monitoring tool can help facilitate data management and analysis activities throughout the investigation. Epidemiologists should analyze data collected from case interviews to determine:

- The magnitude and distribution of the outbreak
- Time, location, and mode of exposure
- Demographics of affected persons

- Vehicle(s) of exposure
- Persons at risk for disease (from either initial exposure or secondarily through contact with a case) who should need treatment, prophylaxis, and medical follow-up.

L. CONTACT TRACING

If the disease is transmissible from person-to-person, those responsible for contact management should endeavor to interview possible contacts identified by cases and those identified through other means (e.g., hotline) to confirm their contact status. All clinical and epidemiologic information should be entered into a database for analysis.

All persons identified as contacts should be referred for vaccination, prophylaxis, isolation and/or quarantine as appropriate and should be kept under active surveillance (temperature checks twice a day) by those responsible for contact management. Contacts that develop fever should be advised to seek medical attention immediately.

Contact management forms have been developed for plague, smallpox, and viral hemorrhagic fevers (VHFs) to help facilitate the management of data from all contacts under surveillance.

Contact tracing guidelines (subject to revision upon release of CDC agent specific guidelines)

	SMALLPOX[7]	PRIMARY PNEUMONIC PLAGUE[8]	VIRAL HEMORHAGIC FEVERS (VHF)[9]
Definition of a contact	A person who has been in the same household as the infected individual or who has been in face-to-face contact with the patient after the onset of fever*. Face-to-face contact is defined as contact with a patient at less than 2 meters (6.5 ft)[10]	A person having had household, hospital and/or face-to-face contact with persons with primary pneumonic plague from the onset of symptoms through completion of 48 hours of appropriate antibiotic therapy. Face-to-face contact is defined as contact with a patient at less than 2 meters (6.5 ft)	A person having had physical contact with a case or the body fluids of a case within 3 weeks after the onset of illness. Physical contact includes sharing the same room/ bed, caring for the patient, touching body fluids, testing patient laboratory specimens.
Temperature checks (2x/day): # days after last exposure to case	17 days	7 days	21 days
Temperature at which contact should seek medical attention	> 100.4° F / 38° C		

*It may be necessary to locate all face-to-face contacts with the case up to 17 days prior to the case's onset of fever for epidemiologic purposes (e.g., to locate all persons who might have been exposed to a common source and who may also be ill or incubating infection)[11].

SOURCE: CALIFORNIA DEPARTMENT OF HEALTH SERVICES

Table 4. Epidemiologic Table (From: California DHS)

M. LABORATORIES

Epidemiologic response personnel should refer questions regarding specimen collection, packaging, storage, and shipment to the appropriate point of contact at the local public health laboratory.

N. EXPANDED SURVEILLANCE FOR NON-HUMAN POPULATIONS

If the disease outbreak is thought to involve animals, public health officials from the

Vector-Borne Diseases Section (VBDS) and Veterinary Public Health Section (VPHS) should coordinate enhanced vector and veterinary surveillance as necessary. The ability of an aerosolized release of a vector-borne bioterrorist agent targeted against

humans to subsequently affect reservoir populations depends on many factors (e.g., specific location indoors or outdoors, geographical location – urban or rural, presence of competent reservoir and vector populations, climatic factors, season, etc.). The actual likelihood of such an occurrence would presumably be low. However, if location and environmental factors were conducive to exposing competent reservoir populations to the bioterrorist agent, it would be prudent to establish surveillance and possible vector control activities.

After an aerosolized release of a vector-borne bioterrorist agent, VBDS could conduct a risk assessment to determine the risk of subsequent vector-borne transmission (by measuring the local vector/reservoir densities and their competencies. This could be very useful for those involved in the managing the bioterrorist event response. Domestic and wildlife populations may experience morbidity and mortality due to bioterrorist agents. If animals are affected in a bioterrorist attack, VPHS should coordinate with New Jersey Department of Food and Agriculture (NJDFA), the New Jersey Department of Fish and Game (NJDFG), and veterinary practitioners to monitor susceptible animal populations and to implement appropriate control measures (e.g., quarantine, treatment, and vaccination) to prevent spread of the disease within animal populations.

O. RECOMMENDATIONS FOR PUBLIC HEALTH ACTION

Experts have compiled consensus treatment and post-exposure prophylaxis guidelines for the top-threat bioterrorist agents. However, in addition to the consensus treatment guidelines, results from analyses of outbreak-specific epidemiologic data should be used to identify the exposed population(s), priority groups for prophylaxis, and the appropriate strategies for quarantine and isolation. This information should be provided to those responsible for coordinating the medical response. The Medical Response Section of the Bioterrorism Preparedness and Response Plan should also contain guidelines and recommendations for disease prevention and control measures, including:

- Treatment of cases
- Prophylactic treatment of exposed persons
- Isolation of cases and quarantine of exposed persons, if necessary

- Use of personal protective equipment (PPE)
- Implementation of infection control practices
- Appropriate handling of the vehicle or source, if necessary

P. OVERT OR ANNOUNCED BIOTERRORIST THREAT

The epidemiologic response to an overt or announced bioterrorism event shall be guided by the FBI and law enforcement assessment of the credibility of the threat. If the FBI believes the threat to be credible and has obtained information about the time, place, mode, and/or contents of the release, this information should be made available by the FBI to public health personnel as soon as possible so that public health can:

- define the population at risk for exposure to the biological agent;
- locate the persons at risk for exposure as soon as possible to assess them for illness and provide appropriate preventive treatment;
- monitor the persons who have received preventive treatment for symptoms or signs of disease; and implement enhanced surveillance for the suspected disease at health care facilities, laboratories, and emergency medical services.

Active surveillance for diseases caused by other potential bioterrorist threat agents should also be conducted, as multiple biological agents may have been released at the same time or serially.

Notification of public health and medical personnel and any release of public information shall be coordinated with the FBI. The epidemiologic investigation shall be coordinated with the FBI's criminal investigation. If cases of illness are found that do not fit epidemiologically with the alleged time, place, or mode of exposure, a full epidemiologic investigation should be conducted to determine the actual time and conditions of exposure, just as if the event had been covert. (After: California Department of Health and Human Services Response Plan).

.

APPENDIX C. (CDC) TOP PRIORITY BIOTERRORISM THREAT AGENTS

A. CATEGORY A

High-priority agents include organisms that pose a risk to national security because they:

- can be easily disseminated or transmitted person-to-person
- cause high mortality, with potential for major public health impact
- might cause public panic and social disruption
- require special action for public health preparedness

Category A agents include:

- Bacillus anthracis (anthrax)
- Clostridium botulinum toxin (botulism)
- Francisella tularensis (tularemia)
- variola major (smallpox)
- Yersinia pestis (plague)
- Filoviruses
- Ebola virus (Ebola hemorrhagic fever)
- Marburg virus (Marburg hemorrhagic fever)
- Arena viruses
- Junin virus (Argentinean hemorrhagic fever) and related viruses
- Lassa virus (Lassa fever)

B. CATEGORY B

Second highest priority agents include those that:

- are moderately easy to disseminate
- cause moderate morbidity and low mortality
- require specific enhancements of public health diagnostic capacity and enhanced disease surveillance

Category B agents include:

- Alpha viruses
- Eastern and western equine encephalomyelitis viruses (EEE, WEE)
- Venezuelan equine encephalomyelitis virus (VEE)

- *Brucella* species (brucellosis)
- *Burkholderia mallei* (glanders)
- *Coxiella burnetii* (Q fever)
- Epsilon toxin of *Clostridium perfringens*
- Ricin toxin from *Ricinus communis*
- Staphylococcal enterotoxin B

A subset of Category B agents includes pathogens that are food- or waterborne. These pathogens include but are not limited to:

- Cryptosporidium parvum
- Escherichia coli O157:H7
- Salmonella species
- Shigella dysenteriae
- Vibrio cholerae

C. CATEGORY C

Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of:

- availability
- ease of production and dissemination
- potential for high morbidity and mortality and major health impact

Category C agents include:

- Hantaviruses
- Multidrug-resistant tuberculosis
- Nipah virus
- Tick-borne encephalitis viruses
- Tick-borne hemorrhagic fever viruses
- Yellow fever

Preparedness for List C agents requires ongoing research to improve disease detection, diagnosis, treatment, and prevention. (After: California Department of Health and Human Services Response Plan).

APPENDIX D. DMIS TOOLS

A. STARTING DMI-SERVICES

The DMI-Services Quick Start screen, which displays at the start of every new DMIS session, can help expedite the process of starting new incidents, alerts, and Instant Message sessions.

Figure 32. DMIS Log In (From DMIS Program)

The 'Quick Start' screen may also be used to review an operator's profile. Locate recently used incidents quicker and easier by using the Most Recently Used (MRU) List. The MRU List allows the operator open and displays the four most recently used Incidents and Alerts. Those COG Operators who frequently send Incidents and Alerts to the same COGs should like the new Distribution Lists feature. Distribution Lists allow an operator to establish a list of COGs to whom new Incidents and Alerts may be sent on a regular basis. In summary DMIs updated release offers:

Journal produces a clean audit trail -- The delete and update features have been removed from Journal function to enable COGs to have a clean audit trail in that Operators cannot alter saved journal entries after the fact.

Expanded list of Incident Types -- When creating a new incident, Operators may now choose from among 28 specific types of incidents.

Improved Incident List -- DMI-Services has added the Last Update/Post Date field to the Incident List for easier sorting.

COG Sorting -- Operators find each other easier in the DMIS Messenger. They can sort COGs in a drop-down list of DMIS Messenger. Now it's easier than ever to find specific Operators quickly.

Web Map Services -- DMI-Services added Iowa's Environmental Mesonet (IEM) RadView Service to Web Map Services. This service, also known as NEXRAD, is a composite radar service updated every five minutes.

Once you installed DMIS you should proceed as follows:

1. Double-click on the DMI-Services icon. The Login screen is displayed.
2. Enter the assigned operator (User) name in the Operator Login Name field.
3. Enter the assigned password in the Password field.
4. When a DMI-Services Operator is a member of more than one COG, he or she may select which COG to log into from a drop-down list.
5. Click the OK button or press the Enter key to log into DMIServices. Once the operator has logged in, the Login screen closes and the DMIS Desktop menu becomes active.

From the DMI-Services menu the DMI-Services operator may access all functionality that the COG Administrator has set for him or her. Permissions are granted based on role.

Figure 33. DMI-Services Menu (From: DMIS Program)

After the operator has successfully logged into DMIS, the 'Quick Start' screen is displayed. 'Quick Start' enables the operator to quickly create new Incidents and Alerts, access and Operator Profile, or start an Instant Messenger session.

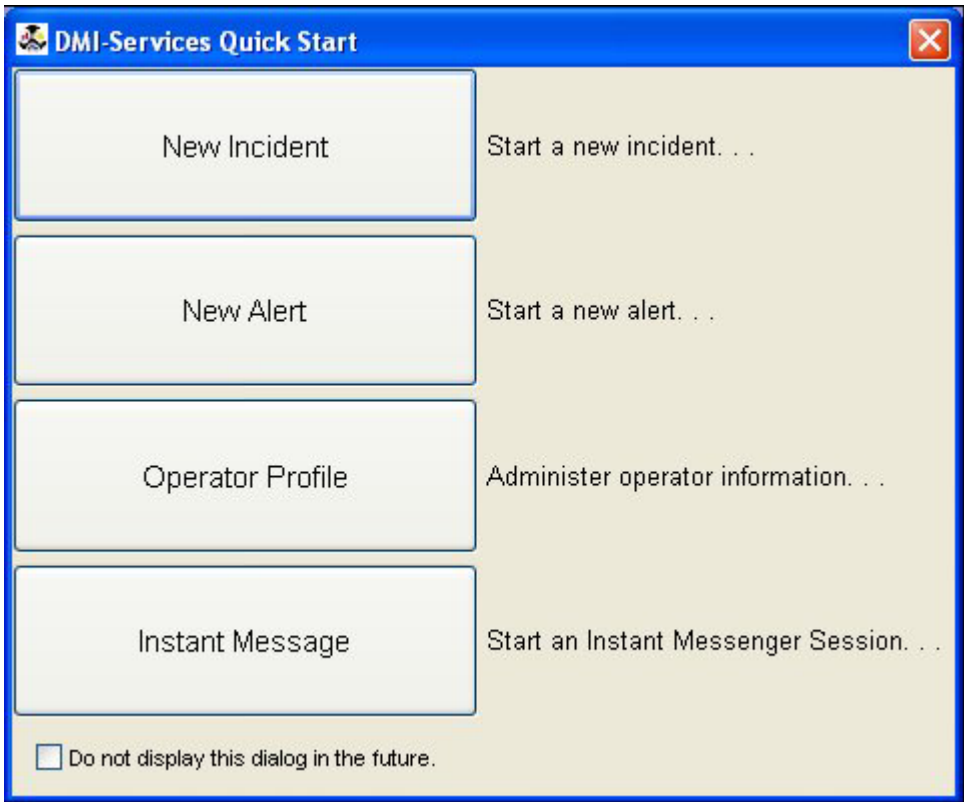


Figure 34. DMI Services Quick Start (From: DMIS Program)

Click on the New Incident button to begin a new incident.

Click on the New Alert button to create a new Alert.

Click on the Operator Profile button to display the Operator Profile screen.

Click on the Instant Message button to start a new DMIS Messenger session.

Upon logging into DMIS, the DMI-Services Operator can access DMIS functions from the **DMI-Services** menu.

Commands in the menus have underlined letters that indicate what keys can be used to perform the action. For example, use **Ctrl + O** to access the **Operator Profile** screen.

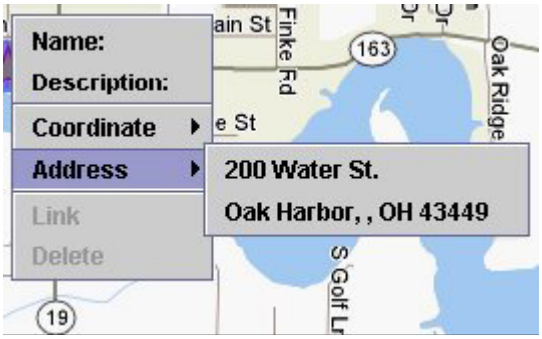


Figure 35. DMI Services (From: DMIS Program)

Logout Menu Option --To log out of DMI-Services, the Operator may use the Logout command accessible under the DMI-Services menu. Administration Menu Option Operators can use the Administration menu, located in the DMIServices menu, to access:

- Settings
- COG Profile
- Operator Profile

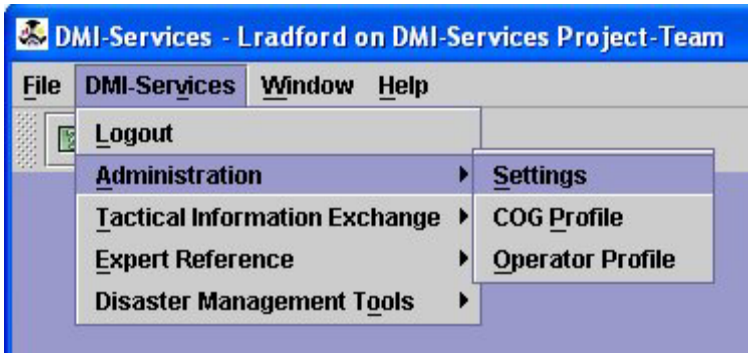


Figure 36. DMI Services (From: DMIS Program)

COG Administrators can use the Administration menu, located in the DMI-Services menu, to access:

- Settings
- COG Configuration
- COG Profile
- Operator Profile
- Reports

B. DMI CAPABILITIES

1. Tactical Information Exchange Menu Option

The Tactical Information Exchange menu, located in the DMIServices menu, enables the DMI-Services operator to access commands for:

- Incident List
- Archived Incident List

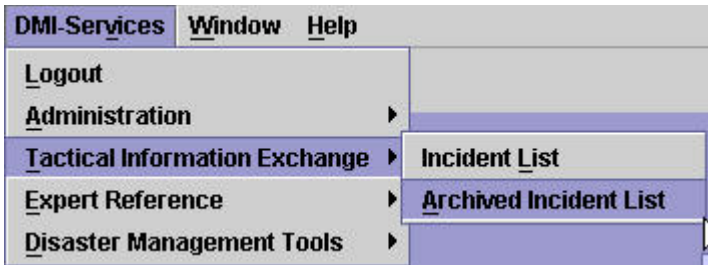


Figure 37. DMI Services (From: DMIS Program)

2. Disaster Management Tools Menu Option

The Disaster Management Tools menu is located in the DMIServices menu. Here the operator can access commands for:

- Web Based Tools
- Disaster Help
- NOAA nowCoast
- NOAA EMWIN
- DMI-Services Home
- National Incident Summary Map
- DMIS Messenger
- Weather Forecast Tool
- Alerts List
- Distribution List

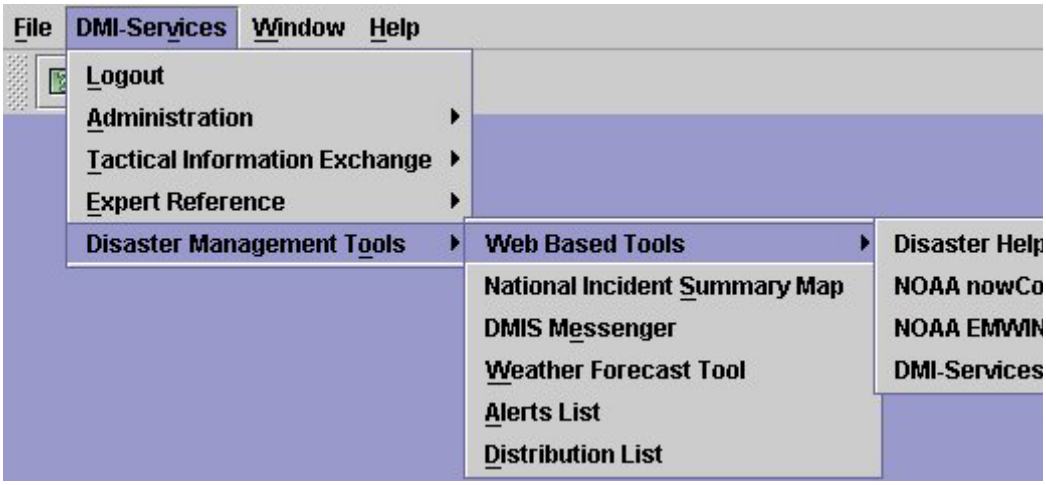
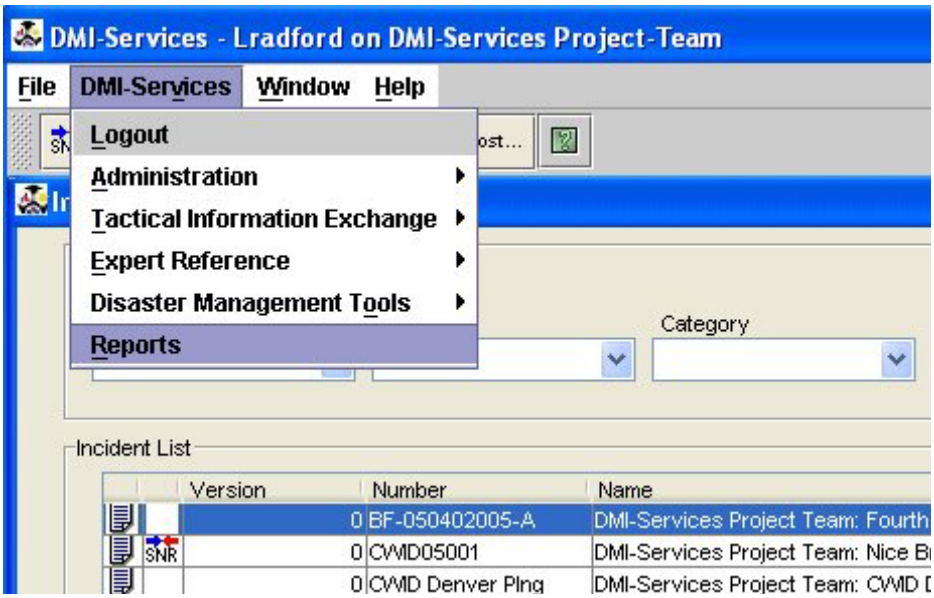


Figure 38. DMIS Management Tools (From: DMIS Program)

3. Reports Menu Option

The Reports menu is only available in the Operator Profile, Incident List, and Incident Information panels. Generate reports by filtering information based on available options.



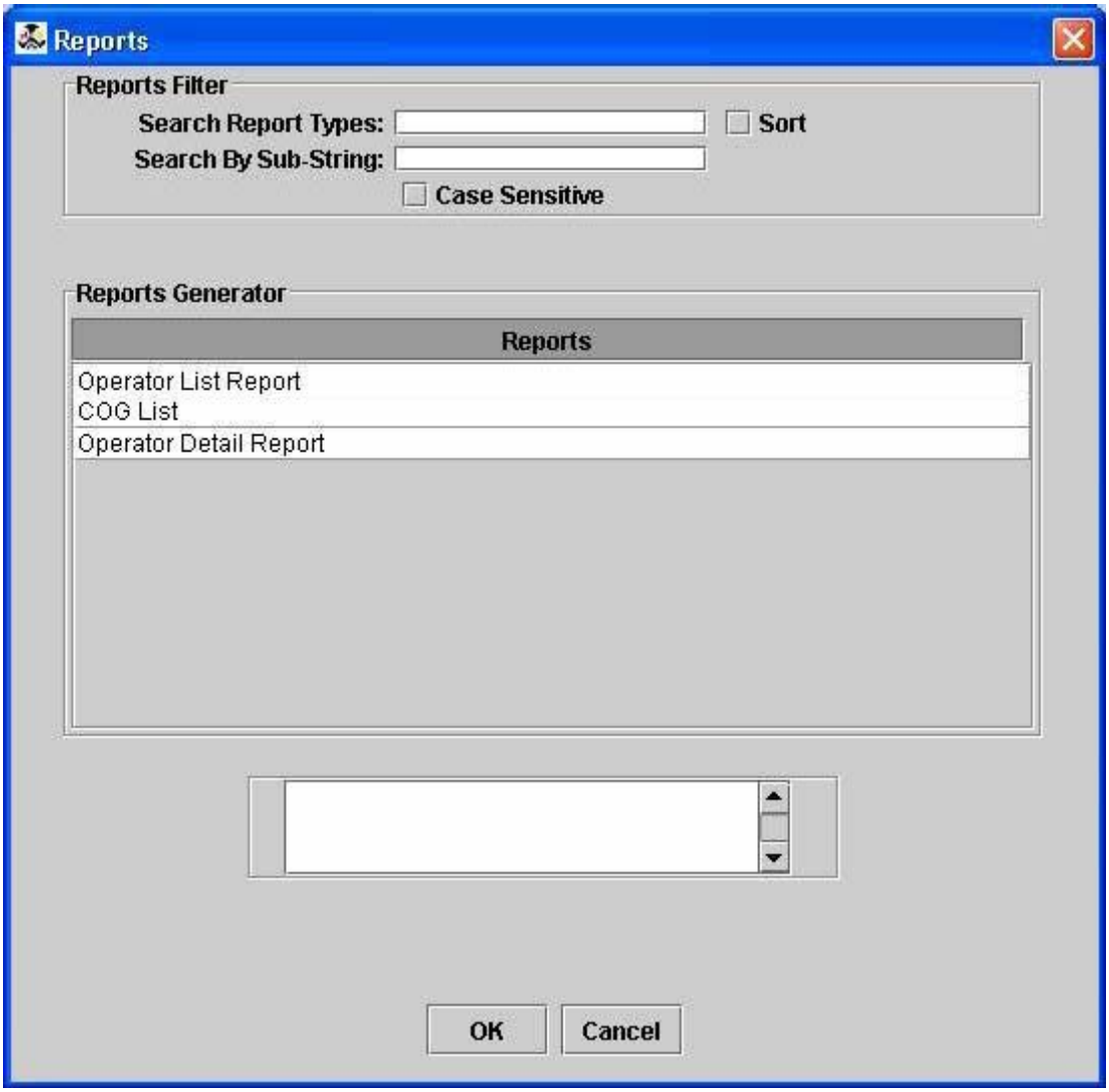


Figure 39. Reports Menu (From: DMIS Program)

4. Using Screen Controls

A DMI-Services screen is made up of different controls, including text boxes, option buttons, drop-down lists, tables, etc. You can use either the mouse or Tab key to move from field to field.

a. Text Boxes

Text boxes hold a limited amount of data. To enter information in a text box, click inside the box and begin typing. Use the Tab key to go from field to field.

Figure 40. Text Boxes (From: DMIS Program)

b. Memo Fields

Memo fields are used for narrative text and can hold several lines of information.

Figure 41. Memo Fields (From: DMIS Program)

c. Radio buttons

Radio buttons are used to select one option from a group of many options. Only one choice can be selected at a given time. To select an option, click the radio button to the left of its description.

Figure 42. Radio buttons (From: DMIS Program)

d. Check-boxes

Check-boxes allow the operator to select more than one choice in a group. The operator can select any number of check-boxes (or leave them blank).

Figure 43. Check-boxes (From: DMIS Program)

e. Drop-down Lists

Drop-down lists enable the operator to select from a pre-set list of entries. Drop-down lists offer flexibility that enables the operator to select a previously-used entry or, in some cases, to add their own entry.

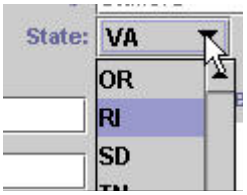


Figure 44. Drop Down lists (From: DMIS Program)

5. Calendars

Calendars are available on many screens to help enter dates.

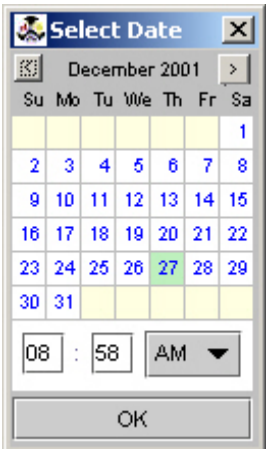


Figure 45. Calendar (From: DMIS Program)

6. Tree View

DMI-Services uses a tree structure in many situations. The tree structure displays the relationship of several items. For example, in TIE the screens for an Incident are represented by a tree structure that makes it easy to move through the screens in any order. For example, to open a screen, click on the paper icon beside the name. To open the Casualties panel, click on the icon next to the word *Casualties*.

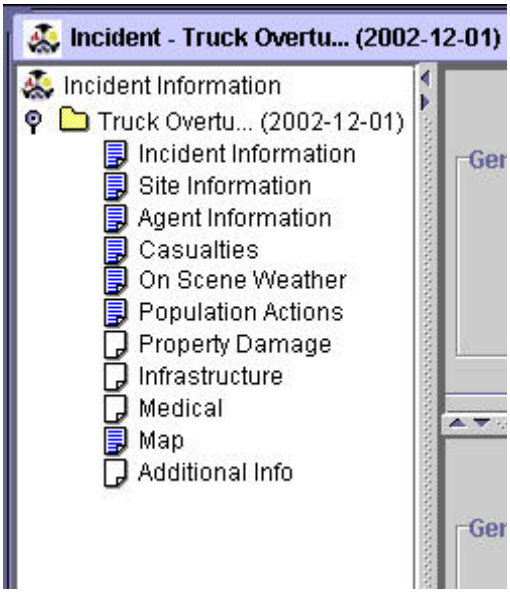


Figure 46. Tree View (From: DMIS Program)

7. Tactical Information Exchange (TIE)

TIE is made up of two major parts: Incident Information and Specific Needs Requests. The incident Information component allows operators to share information about an Incident, including maps, sheltering information, weather, etc. Specific Needs Request provides a means of communicating needs for resources (personnel, supplies, etc.) and of replying to the requests that are made. TIE provides broadly accessible capabilities for exchange of information within and between emergency management organizations. Those already using situation reporting software (such as Computer-Aided Management of Emergency Operations -- CAMEO), as well as those using the TIE application from DMIServices, are able to rapidly develop and exchange Incident Information with other DMI-Services Operators. Using DMI-Services provides Operators with an enhanced ability to present a common operating picture and to improve the overall level of situational awareness of incident conditions. DMI-Services include tools to expedite information exchange about mutual aid, state and Federal assistance, and cascading consequences.

8. Incident List

The Incident List screen is used to access incidents for creation, modification, posting, archiving, and reporting. The top pane of the screen is used to filter the list.

Dropdown lists are used to specify the filter criteria. For more information about filtering the Incident List, see Filtering the Incident List.

Figure 47. Incident List (From: DMIS Program)

The Incident List table in the middle of the screen displays the active Incidents. DMI-Services retrieves and displays an updated Incident List when an Operator:

- Creates a new incident
- Modifies an incident
- Posts an incident
- Archives an incident
- Filters the Incident List by any criteria
- Sorts the Incident List by any of the fields
- Clicks on the Refresh button.
- Each entry or row in the Incident List displays data in the following fields:
- Status/Attachments Icon
- Specific Needs Request
- Version
- Number
- Name
- Category
- Type
- Date, and
- Description.

Icon Status Displays the appropriate icon for the status of that specific incident. See icons.

SNR Icon Displays SNR Icon if a Specific Needs Request has been created and/or posted.

Version Displays the version number for the Incident.

Number Displays the Incident Number.

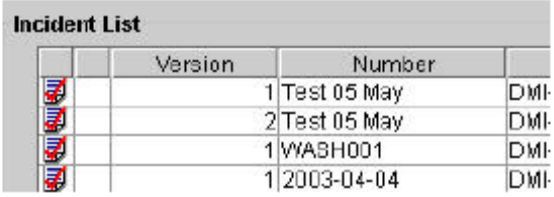


Figure 48. Incident List (From: DMIS Program)

9. Weather Tool

To access the weather tool:

1. Retrieve the Incident List and open the Incident Information panel.
2. From the Incident Information form, select the Weather Forecasts icon to open the panel. The Weather Forecasts panel is displayed.
3. Enter the ZIP Code in and click the Go button. DMIS refreshes the screen to display the forecast for ZIP Code.

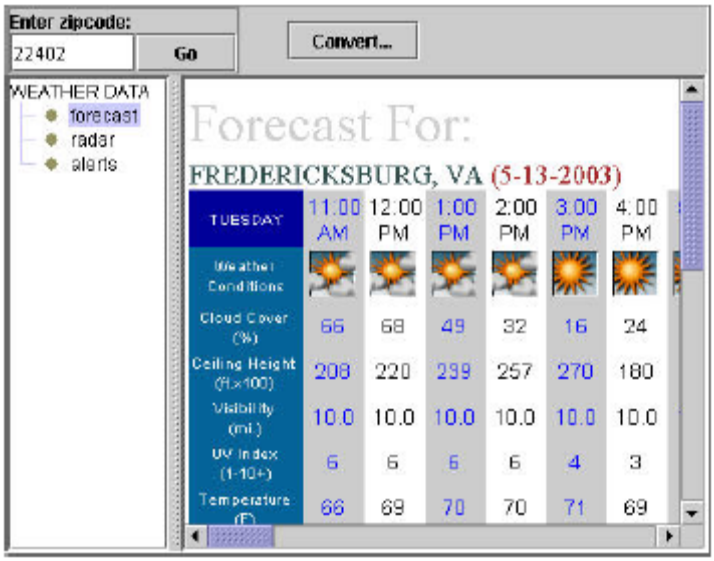


Figure 49. Weather Data (From: DMIS Program)

10. Radar Data

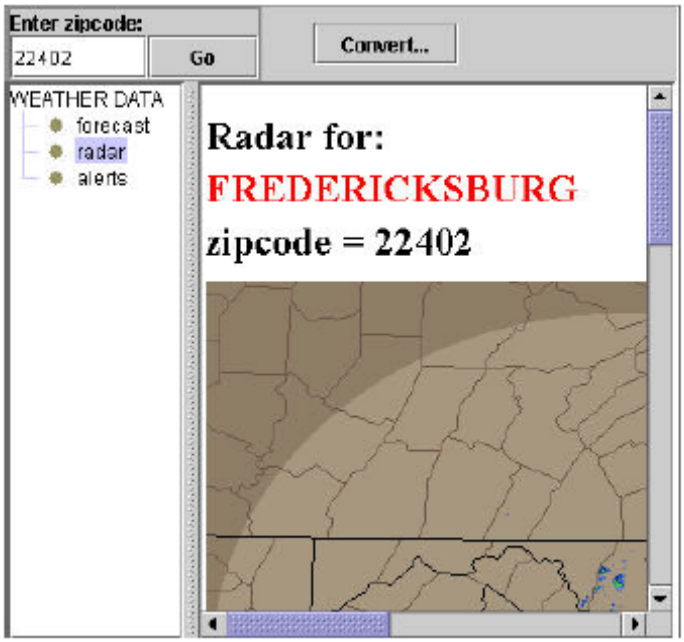


Figure 50. Radar data (From: DMIS Program)

11. Shelter Place

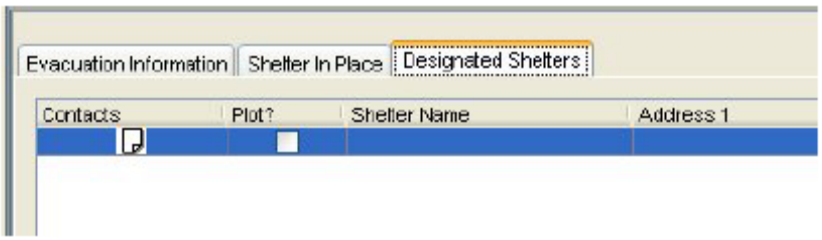


Figure 51. Shelters (From: DMIS Program)

12. Property Damage

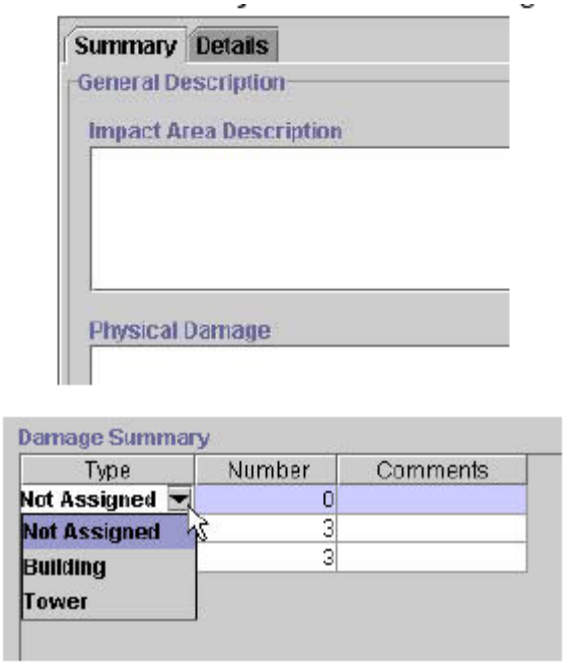
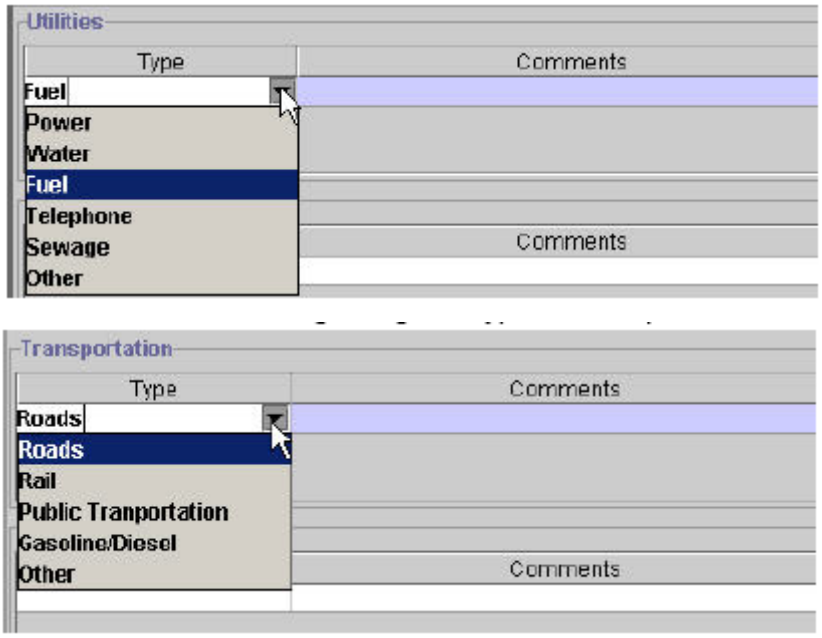


Figure 52. Property Damage (DMIS Program)

13. Infrastructure Information



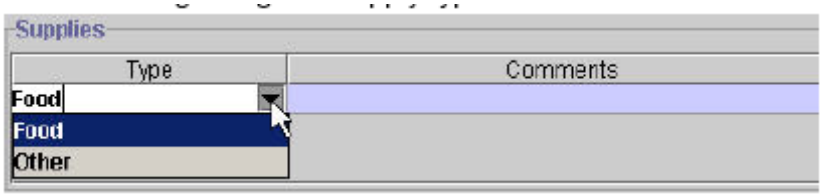


Figure 53. Infrastructure (From: DMIS Program)

14. Medical Information

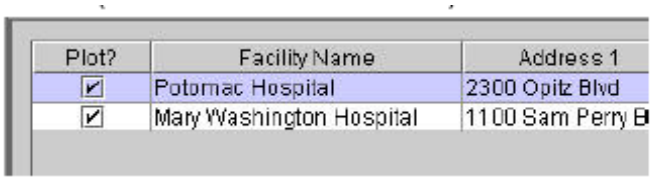
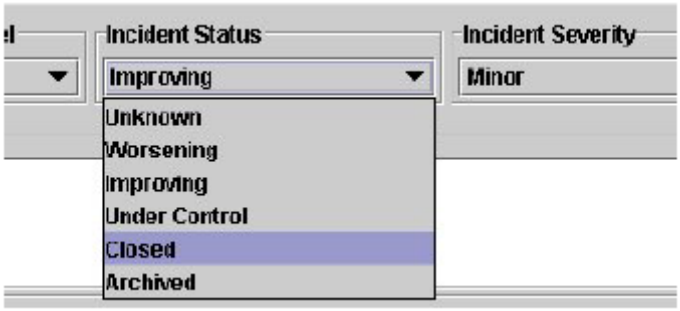
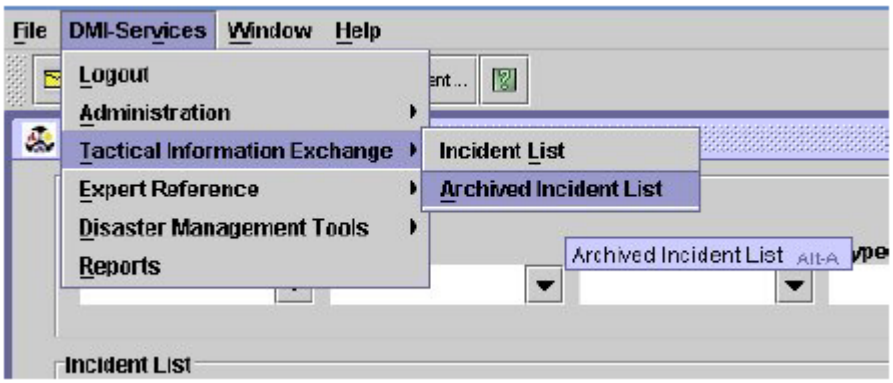


Figure 54. Medical Information (From: DMIS Program)

15. Archiving Incidents





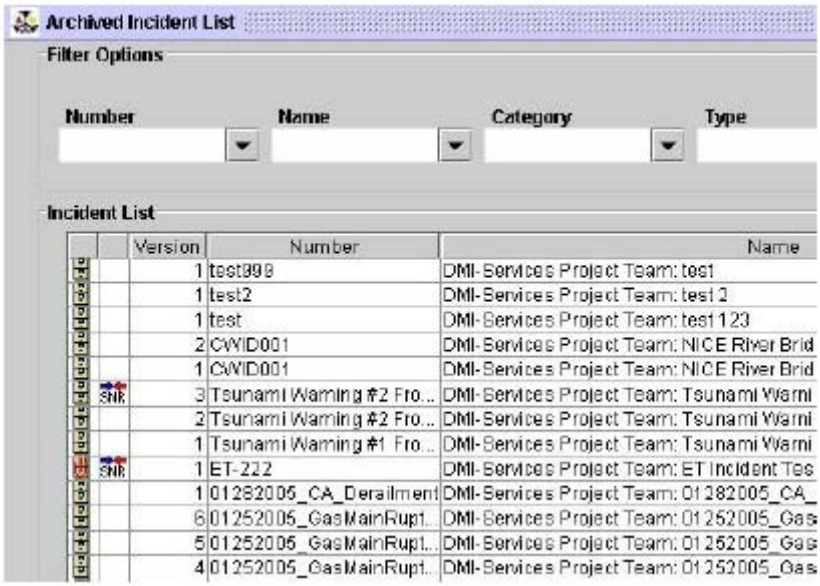


Figure 55. Archiving Menu (From: DMIS Program)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alex Bordetsky
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California

4. Dan Dolk
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California

5. Dan C. Boger
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California