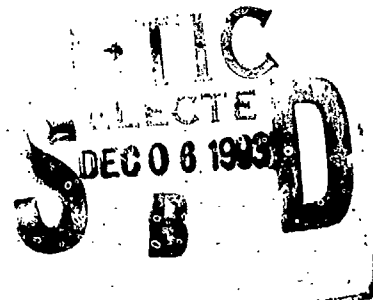# NAVAL POSTGRADUATE SCHOOL
## Monterey, California

AD-A273 432

## THESIS

ANALYSIS OF DISASTER PREPAREDNESS PLANNING
MEASURES IN DOD COMPUTER FACILITIES

by

John D. Harrigan

September, 1993

Principal Advisor:                                    William J. Haga

93-29535

# REPORT DOCUMENTATION PAGE

| 1a Report Security Classification: Unclassified | | 1b Restrictive Markings | | | |
|---|---|---|---|---|---|
| 2a Security Classification Authority | | 3 Distribution/Availability of Report | | | |
| 2b Declassification/Downgrading Schedule | | Approved for Public Release; Distribution is unlimited. | | | |
| 4 Performing Organization Report Number(s) | | 5 Monitoring Organization Report Number(s) | | | |
| 6a Name of Performing Organization<br>Naval Postgraduate School | 6b Office Symbol<br>(if applicable) 37 | 7a Name of Monitoring Organization<br>Naval Postgraduate School | | | |
| 6c Address (city, state, and ZIP code)<br>Monterey CA 93943-5000 | | 7b Address (city, state, and ZIP code)<br>Monterey CA 93943-5000 | | | |
| 8a Name of Funding/Sponsoring Organization | 6b Office Symbol<br>(if applicable) | 9 Procurement Instrument Identification Number | | | |
| Address (city, state, and ZIP code) | | 10 Source of Funding Numbers | | | |
| | | Program Element No | Project No | Task No | Work Unit Accesrion N |

11 Title (include security classification) Analysis of Disaster Preparedness Planning Measures in DOD Computer Facilities

12 Personal Author(s) John D. Harrigan

| 13a Type of Report<br>Master's Thesis | 13b Time Covered<br>From   To | 14 Date of Report (year, month, day)<br>1993 September | 15 Page Count   143 |
|---|---|---|---|

16 Supplementary Notation 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.

| 17 Cosati Codes | | | 18 Subject Terms (continue on reverse if necessary and identify by block number) |
|---|---|---|---|
| Field | Group | Subgroup | Disaster Preparedness Planning in DOD Computer Facilities |
| | | | |

19 Abstract (continue on reverse if necessary and identify by block number)

   This thesis will analyze a disaster recovery plan currently in use at a selected DOD computer facility, as well as investigate facility contingency planning documents actually tested during recent natural disasters. The primary goal of this thesis is to measure the effectiveness of two selected DOD facilities' disaster recovery plans following significant natural disasters, and to study what characteristics of these planning documents were most useful to facility personnel. Equally as important is the analysis of why established plans, or portions of those plans were less than effective. From this appraisal, advantages, disadvantages and lessons learned should assist DOD information managers in identifying and correcting potential weaknesses in their disaster recovery plans.

| 20 Distribution/Availability of Abstract<br>XX unclassified/unlimited __ same as report __ DTIC users | 21 Abstract Security Classification<br>Unclassified | | |
|---|---|---|---|
| 22a Name of Responsible Individual<br>William J. Haga | 22b Telephone (include Area Code)<br>(408) 656-3094 | 22c Office Symbol<br>AS/HG | |

DD FORM 1473, 84 MAR        83 APR edition may be used until exhausted        security classification of this page

All other editions are obsolete

Analysis of Disaster Preparedness Planning Measures
in DOD Computer Facilities

by

John D. Harrigan
Major, United States Marine Corps
B.S., Pittsburg State University, 1980

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT
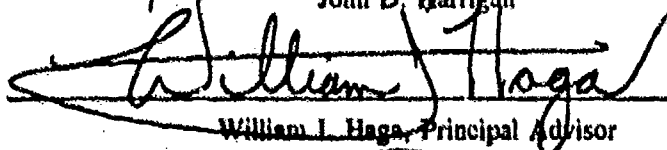
from the

NAVAL POSTGRADUATE SCHOOL
September 1993

Author: _____
John D. Harrigan

Approved by: _____
William L. Haga, Principal Advisor

_____
Roger Stemp, Associate Advisor

_____
David R. Whipple, Chairman
Department of Administrative Sciences

ii

# ABSTRACT

This thesis will analyze a disaster recovery plan currently in use at a selected DOD computer facility, as well as investigate facility contingency planning documents actually tested during recent natural disasters.

The primary goal of this thesis is to measure the effectiveness of two selected DOD facilities' disaster recovery plans following significant natural disasters, and to study what characteristics of these planning documents were most useful to facility personnel. Equally as important is the analysis of why established plans, or portions of those plans were less than effective. From this appraisal, advantages, disadvantages and lessons learned should assist DOD information managers in identifying and correcting potential weaknesses in their disaster recovery plans.

iii

# TABLE OF CONTENTS

# LIST OF FIGURES

## ACKNOWLEDGEMENTS

# I. INTRODUCTION

## A. PURPOSE

The purpose of this thesis is to analyze a disaster recovery (or contingency) plan currently in use at a selected Department of Defense (DOD) computer facility, and compare this plan to recovery plans that have been tested during actual disasters.

Disaster plans, like military preparedness requires an organization to be ready to do what it likely will never do. The plans may suffer from what researchers call predictive validity. In the past five years, the U. S. Department of Defense (DOD) has encountered repeated tests of its Management Information System disaster plans.

## B. OBJECTIVES

A major objective of this thesis will be to discover what makes a disaster recovery (or contingency) plan work and why. Equally as important is the analysis of why established plans, or portions of these plans, were less than effective when used during actual disaster scenarios. Valuable lessons learned could assist computer facility planners in identifying and correcting potential weaknesses in their disaster recovery plans.

1

Computer facility disaster preparedness and related topics are issues often paid little attention by computer facility planners until a natural or man-made disaster occurs. Disasters often strike unexpectedly, as witnessed by: the eruption of Mount Pinatubo and the subsequent abandonment of Clark Air Force Base, Philippines; the destruction of Homestead Air Force Base, Florida and surrounding communities by Hurricane Andrew; and the terrorist bombing of New York's World Trade Center.

These incidents have provided information and lessons learned for contingency planners and information managers, and they have increased awareness levels concerning natural disasters and computer security issues.

## C.  THE NEED FOR DISASTER RECOVERY PLANNING

The need for disaster recovery planning should be apparent to information managers. Not only does disaster planning help to save valuable equipment and jobs, but, more importantly, serves to protect the lives of facility personnel.

### 1.  The Bank of New York

Many organizations pay a heavy price by neglecting to plan for disaster-related computer downtime. Following a 27-hour computer failure at the Bank of New York in 1985, the bank was forced to borrow 22 billion dollars from the discount window of the Federal Reserve Bank. This loan

threw the weighted rate of federal funds out of balance and cost the Bank of New York four to five billion dollars in interest. In addition, senior officials of the bank were summoned to appear before a Congressional investigating committee to explain their lack of foresight in disaster preparedness planning. (Toigo, 1989, p. 11)

### 2. Government Regulations

It is evident that there are monetary penalties for failing to develop and use a disaster recovery plan, but there are U. S. Government regulations that may result in punitive measures a well.

The Foreign Corrupt Practices Act of 1977 states that businesses must take measures to guarantee the security and integrity of assets -interpreted to include accounting and ledger information stored and processed on electronic data processing systems.

The Act provides the capability to prosecute individual managers and corporate executives for failure to plan adequately for a disaster. Individual fines of up to $10,000, five years in prison and corporate penalties of more than one million dollars have been established.

Office of Management and Budget (OMB) Circular A-71

requires government agencies using data processing

facilities to take measures to safeguard these facilities.

Rigidly enforced as a matter of national security, the rule

has been extended to include government contractors and

subcontractors.  (Toigo, 1989, p. 10)

## D.  DISCUSSION

### 1.  Definitions

Toigo defines a disaster as:

> ...an interruption of business due to the loss or denial
> of the information assets required for normal
> operations...a loss or interruption of the company's
> data processing function, or to a loss of the data
> itself.  Loss of data can result from accidental or
> intentional erasure or destruction of the media on which
> data is recorded.  This loss can be caused by a variety
> of man-made or natural phenomena.  (Toigo, 1989, p. 4)

### 2.  Disaster Size and Shape

The term disaster suggests a major calamity--a

terrorist bombing, a hurricane or tidal wave, an earthquake,

perhaps a war--but a disaster can come in many shapes and

sizes.  All disasters may not be on the scale described

above.  An accidental erasure of a hard disk at a small

organization may cause much damage and lead to an

unacceptable interruption of normal business operations.

The potential for lost revenue from an interruption of operations due to a loss of information systems should prompt all organizations, including the Department of Defense (DOD), to adequately train and prepare for a disaster within their facility.

3. **Constants**

There are some constants about disasters. One constant is time. As businesses grow more dependent on customized data processing systems, the timely restoration of system-provided functions is critical.

According to a 1978 study by the University of Minnesota, a data processing failure in a financial institution one-half day in length will degrade normal business activity by 13 percent for the two weeks following the failure. A ten day outage will result in a 97 percent loss of business activity. (Toigo, 1989, p. 5)

Although this thesis concentrates on Department of Defense (DOD) computer facilities, the loss of computer support and data processing capability is still a major issue. Following a disaster, the less than timely resumption of critical computer operations such as aircraft maintenance, air-traffic control and logistics support could result in a loss of lives, revenue and mission capability.

## 4. Coordinated Activities

Toigo defines disaster recovery as an organization's ability to continue day-to-day operations through a series of coordinated activities, despite an occurrence of catastrophic nature.  These activities may include:

- Emergency Action--Procedures for reacting to crises ranging from HALON (fire-extinguishing) activation procedures to emergency evacuations.

- Notification--Procedures for notifying relevant managers in the event of a disaster.  A contact list of home and emergency telephone numbers is usually provided.

- Disaster Declaration--Procedures pertaining to criteria for determining whether the situation is in fact a disaster, assessment of damage following a disaster, and procedures for declaring a disaster and invoking the (disaster recovery) plan.

- Systems Recovery Procedures--Procedures to be followed to restore critical and vital systems at emergency service levels within a specified time frame in accordance with the systems recovery strategy defined in the disaster recovery plan.

- Network Recovery Procedures--Procedures to reinstate voice and data communications at emergency service levels within a specified time frame in accordance with the network recovery strategy defined in the plan.

- User Recovery Procedures--Procedures for recovering critical and vital user functions within a specified time frame in accordance with planned strategy.

- Salvage Operations Procedures--Procedures for salvaging facilities, records and hardware, often including the filing of insurance claims and the determination of the feasibility of reoccupying the disaster site.

- Relocation Procedures--Procedures for relocating emergency operations (system, network and user) to the original or a new facility, and the restoration of normal service levels.

## 5. Phases of Disaster Recovery

There are several distinct phases of disaster recovery. A reference document on disaster recovery planning used terms such as planning, preparation, implementation and recovery to refer to disaster recovery plan formulation and design as well as its implementation. (Hural, 1992, p. 5)

In contrast, Toigo uses the phrases evacuation, recovery and relocation/reentry in reference to the reaction and recovery from an actual disaster, and assumes that a disaster recovery plan is already in place.

Discussion is required on each of these phases as they relate to fundamental portions of disaster recovery planning:

Planning Phase--This phase of the disaster recovery plan is used to develop the programs, policies and procedures to be put into operation to reduce the effect of a natural disaster on an organization's information system.

Preparation Phase--The preparation phase implements the procedures identified by the requirements in the planning phase, including actions to be taken in the event that advance notification of an impending disaster is available. It also contains standard procedures to be followed on a daily, weekly and monthly basis in order to be prepared should a disaster occur without prior or advance notice. Its stated purpose is to allow the organization to

7

respond to the impending threat of a disaster, and includes a physical inventory of organizational assets, a risk assessment in order to determine the threats to an organization's information system, alternative technologies that can be used in the event of a disaster, and disaster recovery team iden_ification and training.

Implementation Phase--This phase of the plan describes the procedures to be followed when it has been determined to initiate the disaster recovery plan. The implementation phase moves the organization from the non-critical preparation phase into the full scale emergency activation of the disaster recovery plan. Similar to the mishap plan found in Naval aviation aircraft squadrons, it should be a detailed document with precise steps to follow in the event of an emergency.

This phase is the litmus test as to the overall effectiveness of an organization's disaster recovery planning. To be successful at this phase, the plan must be easy to read with clear objectives, have disaster teams identified and ready to proceed with their stated tasks, and contain enough information so that a backup/alternate user will be able to successfully follow the directions contained within the plan.

Recovery Phase--This phase of plan development outlines procedures that will be performed to return the organization to its original operating level after a disaster has occurred.

Evacuation Phase--This segment of the plan concerns the first three sections of the activities listed above. The evacuation phase contains procedures for reacting to a crisis, notifying personnel in the event of a disaster, determining if a disaster should be declared and implementation of the disaster recovery plan.

Recovery Project or Phase--This phase covers the coordinated activities listed below:

- Critical systems are restored at reduced performance levels.

- Voice and data communications are reinstated at emergency levels.

- Vital user functions are recovered.

- Facilities, records and hardware are salvaged, all within a specified time frame.

Relocation Project or Phase--Contains procedures for relocation emergency operations (system, network and user) to the original or new facility. The new facility may be a "cold site" (a site with little or no existing hardware and equipment), or a "hot site" (an existing computer facility, fully equipped and ready to conduct operations).

## E. METHODOLOGY

Disaster preparedness in the commercial sector is examined in the World Trade Center segment of this thesis. Emphasis is placed on the terrorist incident's impact on personal computer users, local area networks and backup procedures used by affected firms.

Also studied are Clark and Homestead Air Force Bases, two DOD installations whose computer facilities' contingency plans were tested by natural disasters. Toigo's three disaster phases provide the structure for an examination of planning and recovery methods associated with these incidents.

The DFAS/DITSO Kansas City, Missouri contingency plan serves as a model for a detailed analysis conforming to an outline of a generic disaster preparedness plan.

Sources of information include interviews, topical publications, magazine articles, DFAS/DITSO Kansas City's contingency plan and written accounts by participating personnel.

Information pertaining to the two U. S. Air Force Bases was largely obtained during interviews with participants due to a scarcity of official documentation. Most of the Clark AFB disaster plan was lost following closure of the base; Homestead's contingency documentation was destroyed during the disaster. Discussions with DFAS/DITSO Kansas City contingency planners, employees and other facility personnel

aided in the preparation of the contingency planning model.

While in the process of obtaining information, several interviewees requested that they remain anonymous, and were not referred to by name within the thesis.

## II.  WORLD TRADE CENTER INCIDENT

### A.  MULTI-LEVEL PLANNING

The bomb explosion at the World Trade Center emphasizes the need for disaster planning at all levels of computing--from the mainframe down to the individual personal computer (PC) user.  Offices in the Trade Center that used disaster recovery plans experienced short computer downtimes and minimal lost productivity as a result of the bombing. (Fisher, 1993, p. 10)

Kemper, a Chicago-based securities firm, had a backup plan to protect vital data processed by its World Trade Center office.  Nightly, Kemper automatically transferred copies of data stored by its three IBM computers to a backup computer located in Milwaukee, Wisconsin.

When Kemper employees reported for work at a temporary work location on the Monday following the explosion, their customers' vital records were safe, and work resumed with little interruption.  (Fisher, 1993, p. 10)

## 1.   Personal Computer Disaster Recovery

However, not all Trade Center-based firms' computer operations escaped the blast.   PC users suffered losses in productivity during the period immediately following the explosion.   Four days after the incident, as firefighters sifted through the debris, office workers tried to rescue PCs from their ravaged workspaces.   (Fisher, 1993, p. 11)

Tom Abruzzo, senior project manager for Contingency Planning Research Inc., stated:

> ...mainframe and mini (computer) users have hot sites to recreate their operations, but most PC users don't have any idea of what to do if they have no access to their computer.   (Fisher, 1993, p. 11)

An unidentified PC user said:

> Every night, I'm putting a backup tape in my pocket and taking it home.   (Fisher, 1993, p. 11)

### a.   PC and LAN Lessons Learned

Some PC local area network (LAN) managers and users learned valuable lessons from the World Trade Center bombing.   Kenneth Horner, a partner at Deloitte & Touche in the Trade Center's Tower No. 1, was at lunch when the bomb went off.   The Big Six accounting firm evacuated its people from floors 93 to 101 and soon began shifting operations to a company site in mid-town Manhattan.   "We had a disaster recovery plan in place and contingency planning for several clients and ourselves," Horner said.

Returning to the office as soon as possible after the explosion, employees were able to retrieve hard disks and some network file servers from Tower No. 1. Using network-compatible Macintosh computers, disabled LANs were restored fairly quickly. By Monday morning, three days after the blast, Deloitte & Touche was back up and running. Horner stated: "We had a loss of productivity and a large amount of expense, but no client problems." (Leeke, 1993, p. 8)

### 2. Distributed Architectures

The majority of operations that were disrupted by the bombing of the World Trade Center were based on distributed systems and local-area network topologies. This has led information systems executives and industry observers to speculate that the incident will force companies to pay even greater attention to protecting mission-critical applications on distributed architectures. (Hoffman, 1993, p. 67)

The Chase Manhattan Bank was forced to transfer 100 financial services employees and reroute phone lines to the Chase Plaza and other New York locations after the bomb blast. Craig D. Goldman, senior vice president and chief information officer said:

> There's no question that anytime you have a disaster like this, people become much more aware of the rigors of protecting distributed technology... (Hoffman, 1993, p. 67)

14

Most large Trade Center companies with past disaster recovery experience successfully carried over their expertise to distributed architectures preceding the World Trade Center bombing. However, smaller firms with no prior experience were less fortunate. (Hoffman, 1993, p. 67)

### 3. Backups

The New York Clearing House Association (NYCH), which clears billions of dollars in international transactions for member banks daily, had ten members in the Trade Center when the bombing occurred. Four of those banks ended up using NYCH backup facilities in Manhattan to complete $90 billion dollars in transactions on the day of the bombing. (Hoffman. 1993, p. 67)

Tari Schroeder, chief executive officer at Contingency Planning Research, Inc., stated that, based on early investigations among World Trade Center tenants, most of the organizations that suffered data losses or disruptions to distributed systems were backing up data only on a weekly or monthly basis. (Hoffman, 1993, p. 67)

According to Jerome J. Jordan, vice-president of computer operations for the Trade Center-based Commodities Exchange, Inc. (Comex), all trading information is "shadowed" or backed up and routed over an LU6.2 protocol network to computers at a backup facility. As a result, Comex did not lose any data. (Hoffman, 1993, p. 67)

## III. CLARK AIR FORCE BASE INCIDENT

### A. BACKGROUND

Clark Air Force Base (AFB), located on the island of Luzon, Republic of the Philippines (RP), was regarded as paradise by most of the U. S. Air Force personnel fortunate enough to be assigned there. Lush tropical surroundings, a friendly native population and a low cost of living helped make Clark a near-ideal duty location for its American occupants.

The base enjoyed a long and colorful history. Clark was originally founded as Fort Stotsenberg in 1903, following the United States' possession of the Philippines after the Spanish-American War. Much of General Douglas MacArthur's ill-fated Philippine Air Force was destroyed at Clark AFB by the invading Japanese during the dark days of late December, 1941. Thousands of U. S. servicemen spent a few wild days of Rest and Recreation (R&R) from the Vietnam War at Clark and its adjacent Philippine community, Angeles City.

More recently, Clark housed the personnel, aircraft, and equipment of the U. S. 13th Air Force, the 353rd Operations Wing, other supporting units, and thousands of dependent family members.

It was a life in paradise that, as of April 2, 1991, could be measured in days, for Clark AFB lay ten miles from a long-dormant volcano named Mount Pinatubo.

## B. "BLACK SATURDAY"

The beginning of the end of the U. S. Air Force's presence at Clark AFB came on Saturday, June 15, 1991, at 5:55 a.m. local time. In the months since, a skeleton crew left there as caretakers has begun calling that day "Black Saturday". Those who were there say that what they saw will stay with them all their lives.

At that hour came the explosion of Mount Pinatubo, which took place at the same moment that a violent tropical storm, Typhoon Yunya, was sweeping in from the sea and bearing down on the Philippine Islands. Witnesses say they saw a wall of ash and soot some five miles wide rising directly into the typhoon's swirling winds and rain.

Rather than continuing to climb, as did the smaller plumes of previous days, the debris from this eruption began spreading horizontally. Clark AFB lay directly in its path.

At Clark, U. S. Geological Survey (USGS) volcano experts warned Air Force officials that the base could be threatened by pyroclastic flows--streams of molten ash and rock superheated to 900 degrees Celsius and moving at speeds of up to 100 miles an hour. Most of a 1,500-member, mission-essential Air Force team was evacuated to safety at an

agricultural college on the Philippine-controlled portion of
the base.  Only a few members were left at Clark in the
early afternoon, when the sky turned black and it began
raining stones.

"They were just like hailstones.  It was incredible,"
said SMSgt Arthur Futch, a member of the Air Force's
mission-essential team who stayed at Clark throughout the
initial evacuation and its months-long aftermath.  Falling
rocks and ash muffled all sound.  Sergeant Futch said it
"was like a reverse snowstorm," a winter scene with
everything turning black instead of white.

By 2:30 p.m., the situation for those still at Clark
proper was clearly untenable.  All remaining personnel were
taken to the agricultural college.  A natural disaster had
just forced the U. S. to take the unprecedented step of
mounting a complete, immediate evacuation of a major
military installation, leaving behind hundreds of millions
of dollars' worth of equipment and personal possessions.

When the worst part of the ash fall was over, 100
buildings at Clark had been destroyed and the base had
sustained more than $300 million in damage.  (Grier, 1992,
p. 56)

## C. "ERUPTION OF THE CENTURY"

Filipino victims who dwelt near the volcano recalled that the erupting volcano sounded like an enormous stampede was occurring. The earth shook. Ash clouds billowed miles into the sky, transforming day into night. Lahar (volcanic mud) coated the surrounding countryside, destroying thousands of homes, roads, and bridges in the central Luzon plain.

The eruption drove the Aetas, a Stone Age-like tribe virtually untouched by modern civilization, from the mountain craters in which they had lived. Driven into the lowlands by the volcano, they quickly fell prey to diseases, contracted from their new environment, for which they had no natural immunity. Many died, refusing medical care. (Dacaney, 1991, p. 20)

After the Pinatubo eruption, many Filipinos claimed that God punished the Philippines because of the U. S. bases. "The U. S. war facilities helped in the transformation of Olongapo and Angeles into sin cities," insisted Lita Tabelan, a 22-year old Filipino. "What happened to us during the eruption was similar to what happened in Sodom and Gomorrah."

Another Filipino was convinced that the Pinatubo eruption was God's punishment for sinners. "Look at what happened to my neighbor," a 33-year old resident of a small Luzon farming community said, "He has plenty of wives. It must be the reason why his house was totally destroyed during the eruption." (Dacaney, 1991, p. 54)

## D. THE "RING OF FIRE"

Mt. Pinatubo was considered one of the least active volcanos in what volcanologists call the Pacific "Ring of Fire," a belt of seismic activity stretching from Japan southward. Though it was one of the least active, Pinatubo was by no means considered less dangerous.

According to data from the Smithsonian Institution's Global Volcanism Network, eleven of the fourteen largest eruptions of the last two hundred years involved long-dormant volcanoes, including the deadliest eruption of modern times, the 1883 eruption of Krakatoa, which killed 36,000 people in what is now Indonesia. (Grier, 1992, p. 58)

Geologically, the Philippines is one of the most active areas of the world. In July 1990, an earthquake killed 1,621 people on Luzon, and scientists from the Philippine Institute of Volcanology and Seismology think this tremor may have acted as the trigger that helped Pinatubo go critical.

The first hints that something was amiss with the mountain came in the early spring of 1991. On April 2, an explosion from Pinatubo's southern region spread ash across the countryside up to ten kilometers away from the mountain. (Grier, 1992, p. 58)

## E. AIR FORCE REACTION

Concerned about Philippine scientists' reports of "seismic swarm" tremors and indications of rising molten lava around Mt. Pinatubo, U. S. Air Force officials requested expert help from the U. S. Geological Survey. Within days after arriving on April 23, a USGS team reported that a major eruption was imminent, but were unable to predict the exact date.

Throughout May 1991, seismic tremors in the Pinatubo region grew stronger, appearing to emanate from points closer to the surface. By early June, experts warned that a major explosion could occur at any time. (Grier, 1992, p. 58)

## F. "FIERY VIGIL"

Alarmed by increasing volcanic activity, Clark AFB officials began preparing for evacuation. By June 8, each American household had received a detailed evacuation pamphlet, giving instructions on what to do, what to bring, and what to leave behind.

Air Force aircraft were the first items to go.  Although the Air Force's drawdown had removed two squadrons of fighter jets from the base, many aircraft remained to be flown out.  On Sunday, June 9, just about everything left on the Clark flight line--helicopters and transport aircraft-- moved to Cubi Point Naval Air Station, minutes away by air on Luzon's Bataan Peninsula.

By early morning on June 9, USGS experts predicted a major eruption within twenty-four hours.  Two hours later, Pinatubo spat ash and rocks skyward.  Although the debris was carried away from Clark, the Base Commander ordered a general evacuation of all married servicemen and women, their families, and other "non-essential" personnel. (Grier, 1992, p. 58)

After several false alarms, the evacuation announcement was broadcast at 5:00 a.m. on June 9 by the base's Armed Forces Radio Network.  By 6:00 p.m. the first of three organized convoys of Clark residents had formed up to transit the fifty-mile, two-lane road to the U. S. Naval Base at Subic Bay, also on the Bataan Peninsula.  Left behind at Clark were 1,500 "mission-essential" personnel, slightly more than half of them Air Force security policemen.

Among the convoy to Subic Bay was Air Force MSgt Joseph Licci, Chief of the Data Processing Center (DPC) at Clark AFB, and his family. Remaining at Clark to operate the DPC were five unmarried Air Force Data Processing technicians: SSgt Charles Reidy, in temporary command of the Center, and four other airmen. MSgt Licci and SSgt Reidy were two major sources of thesis information about U. S. Air Force contingency planning efforts at Clark AFB during the Mt. Pinatubo disaster.

This mass withdrawal, code-named "Fiery Vigil", saw 14,000 Americans move from Clark to relative safety at Subic Bay. Most of them would never return.

On November 26, 1991, after months of unsuccessful negotiations with the Philippine government over the continued presence of U. S. bases in the Philippines, Clark AFB was turned over to the Filipinos. (Grier, 1992, p. 56)

## G. CLARK AFB DATA PROCESSING CENTER

Operating 24 hours a day, seven days a week, the Clark AFB Data Processing Center (DPC) provided mainframe computer support to all host/tenant organizations at the base. Other commands also used the Clark DPC: Camp Wallace Air Station, Camp O'Donnell, and the American Embassy at Manila.

Sixty on-base customers and 300 user terminals were served by the DPC's Sperry S1100/60 mainframe, including: Aircraft Maintenance, Military and Civilian Personnel, Merchandise Control and Accounting/Finance. An on-site tape library provided secure storage for over 5000 magnetic disk tapes.

The Center had an Uninterruptable Power Supply (UPS) to provide emergency power to the mainframe and environmental control systems should the primary electrical power source be interrupted. (Interview, MSgt Licci, USAF, 1993)

## 1. Data Backup and Off-Site Storage Procedures

Off-site storage for backup computer tapes was located in a secure, climate-controlled building miles from the DPC on the opposite side of Clark AFB. The backup tape library consisted of 110 tapes containing current program files and user databases.

As required by Air Force Regulation 700-7, full system backups were performed on a weekly basis. "SAVEALL" tapes, magnetic tapes containing the previous week's data transactions, were unloaded from the mainframe computer and moved to off-site storage the following day. New SAVEALL tapes were then inserted for backup of the current week's processing activities.

Release tapes, tapes containing applications program updates from the Air Force's Standard System Center were also maintained in off-site storage.

To augment the weekly SAVEALL backup routine, nightly "SAVE" backups were performed and transported off-site. SAVEs recorded only databases updated during the day's activities. SAVE and SAVEALL procedures combined to give the Clark DPC a complete backup of all daily and weekly data transactions. (Clark AFB DPC Operating Instruction 123-1, Disaster & Emergency Plan, 1988)

In addition to backup tapes, the DPC also stored copies of their Operating Instructions (OI), contingency plan, extra paper, diskettes, and office supplies for emergency use.

## 2. Transportable Shelter System

Until the spring of 1991, a mobile, self-contained mainframe computer, the Transportable Shelter System (TSS) was located at the Clark DPC. Should Clark's Sperry S1100/60 mainframe computer be rendered inoperative for a prolonged period, the TSS was designed to function as the DPC's alternate processing site.

Contained in four shelters, the TSS also housed user terminals, peripheral devices air-conditioning/humidifier units and three electrical power generators.

The TSS was removed in February 1991. After the TSS departed, the Clark DPC was forced to relocate to other Air Force DPCs to satisfy its alternate site processing requirements. (Interview, MSgt Licci, USAF, 1993)

## H. CLARK DPC CONTINGENCY PLANNING

### 1. Pre-Disaster Planning

The Clark DPC had prepared a contingency plan prior to the Pinatubo disaster. Labeled the Disaster and Emergency Plan (D&E), the document was designed in accordance with Air Force 700 Series Regulations. These regulations require that data processing centers have D&E plans that address real and potential threats to facilities and personnel.

As part of plan preparation, a detailed risk analysis was performed. Natural disasters identified as threats were: fires, floods, severe storms, earthquakes and typhoons. Volcanoes were not considered a plausible threat to the facility. MSgt Licci stated:

> In April '91 the volcano started smoking. Not too many people thought much about it at first. Then it started smoking more and more, and folks became alarmed. In mid-May it started to discharge grey smoke, and base officials called in some volcano experts. (Interview, MSgt Licci, USAF, 1993)

Noting Clark AFB's mounting tension over the restive mountain, Licci began a review of the DPC's contingency documents. MSgt Licci:

> I started a review of our D&E plan, and reviewed all our OIs. I guess we at the DPC had good timing, because between February and May 1991 we had initiated a complete rewrite of all our contingency documentation. We were pretty current on our procedures when the mountain started to get worse. (Interview, MSgt Licci, USAF, 1993)

### 2. Volcano Readiness Levels

In May 1991, the Clark AFB Disaster Preparedness Office, an Air Force agency dedicated to overall base disaster readiness and contingency planning, distributed volcano guidance to all host/tenant commands, uniformed personnel and dependents.

The booklet described five levels of volcanic activity, listed below:

- Level 1--No immediate danger of eruption, volcano not smoking.

- Level 2--Increased danger of eruption, volcano smoking.

- Level 3--Danger of eruption within two weeks.

- Level 4--Danger of eruption within two days.

- Level 5--Danger of eruption within hours/actual eruption.

The Clark DPC, along with all other tenant commands, tailored their disaster preparedness measures to conform to these volcanic activity le Is.

28

By the time these checklists were printed and
distributed throughout the base, Pinatubo was ominously
smoking, and Clark had been placed into a Level 2 readiness
condition.  (Interview, MSgt Licci, USAF, 1993)

### 3. The "Volcano" Plan

As the DPC had no procedures regarding volcanic
activity, MSgt Licci quickly prepared a "Volcano" plan.
Drafted during Clark's Level 2 volcano readiness condition,
this improvised plan contained volcano-specific procedures
and would augment the existing contingency plan.

Using his in-depth knowledge of DPC operations, MSgt
Licci tailored the Volcano Plan to take advantage of the
DPC's strengths: experienced personnel, a proven data backup
system, secure off-site storage and available alternate
processing sites.

#### a. *Final Preparations*

When Level 3 was announced, the DPC made final
preparations for the imminent eruption.  Essential and non-
essential personnel were chosen and briefed.  Specialized
processing teams were formed.

Five unmarried airmen were classified as
essential, and were to continue operations at the DPC after
the general evacuation.  Non-essential personnel and their
families would evacuate when directed.

Several DPC members were designated as the alternate site processing team. Alternate processing sites were informed of the current situation; off-site processing agreements were reviewed and updated. Clark's primary alternate processing site was Kadena AFB, Okinawa. Secondary sites were Yokota AFB, Japan or Osan AFB, Korea. (Interview, MSgt Licci, USAF, 1993)

### 4. Plan Innovations

Due to the rapidly-deteriorating situation and lack of volcano-related procedures, DPC personnel had to innovate and plan "on the fly".

MSgt Licci:

> ...if/when the volcano went off, we wouldn't have the time to go to the off-site tape library, get the tapes and boogy before it was too late, so I initiated a change to our (D&E) procedures. (Interview, MSgt Licci, USAF, 1993)

Using six large (3'x3'x3') aluminum containers left over from the Transportable Shelter System (TSS), DPC personnel retrieved the most current backup tapes from storage, placed them into the airtight containers and secured them within the DPC. Backup tapes stored inside the containers were updated daily. Copies of contingency documentation, personnel rosters and extra supplies were also sealed inside the containers.

Should the volcano erupt, these "bug-out kits", as they were called, would be loaded onto an Air Force vehicle and moved as far from danger as possible, for eventual air transport to an alternate processing site. An escape route was formulated and rehearsed, and the vehicle kept in readiness for the operation. (Interview, MSgt Licci, USAF, 1993)

### 5. Evacuation

The Volcano Plan called for migration to an alternate site when Level 4 conditions were placed into effect. To prepare for this eventuality, MSgt Licci ensured that:

- Temporary duty (TDY) orders were prepared for the alternate site processing team.

- Kadena AFB was notified of the team's impending arrival.

- Team members were briefed and prepared to travel to the alternate site.

- Satellite communications with alternate sites had been tested using the base's fixed SATCOM facility.

However, when Level 4 came into effect a senior DPC official altered the Volcano Plan, cancelling the alternate site team's move to Kadena AFB. Soon after, on June 9, the general evacuation took place. (Interview, MSgt Licci, USAF, 1993)

## I. EVACUATION PHASE

With non-essential personnel evacuating to Subic Bay,
Air Force SSgt Charles Reidy, assisted by four other airmen,
was nominally in charge of the Clark DPC. Data processing
operations resumed at reduced levels due to the limited
number of Center personnel remaining and the departure of
most of the DPC's customers. Backup tapes were updated
daily, secured in the "bug-out kits" and locked in the DPC
supply room.

Everything pertaining to the Volcano and D&E plans had
been accomplished. All that remained was to continue daily
operations, subsist on Meals Ready-to-Eat (MRE) and wait for
the volcano to erupt. It was not a long wait. (Interview,
SSgt Reidy, USAF, 1993)

### 1. Pinatubo Erupts

Unknown to SSgt Reidy and the other remaining Air
Force personnel at Clark AFB, the pressure inside Pinatubo
kept building. On Wednesday, June 12, it blew a column of
ash into a mushroom cloud 60,000 feet high. Most of the
mission-essential crew were moved to temporary safety at the
Pampanga Agricultural College on the slope of Mount Arayat,
several miles from Clark AFB. Luckily, the ash drifted away
from Clark. Over the next few days, however, threatening
seismic activity caused base personnel to sound eight

32

premature evacuation sirens, only to reverse each order within a short time. (Grier, 1992, p. 59)

SSgt Reidy, on duty at the DPC, stated:

> The first time we were ordered to evacuate (June 12), we shut down the facility using emergency power down procedures found in the D&E plan. We grabbed the backup tapes, jumped in our vehicle and ran.... (Interview, SSgt Reidy, USAF, 1993)

After returning to the Center, SSgt Reidy restored power to the mainframe and attempted to resume processing. Immediately, minor problems developed. Magnetic tape "diskpacks" (tape storage and retrieval devices) failed to operate correctly, due to the instantaneous removal of electrical power caused by the emergency power down procedure. Although this condition had been encountered before during practice exercises, SSgt Reidy elected to follow the Volcano Plan and use normal power down procedures for the next actual (or premature) evacuation.

On June 15 came Black Saturday and the freak combination of massive volcanic eruption and typhoon. After four premature evacuations on Saturday alone, the volcano finally left no doubt as to the necessity of moving Clark's remaining Air Force personnel to safety.

SSgt Reidy:

> When the volcano really blew (June 15) we loaded the backup tapes from the supply room and left. The Volcano Plan called for us to leave the mainframe operating to get away from problems with disk storage. Peripheral devices were powered down using normal procedures. I had a feeling we wouldn't be back. (Interview, SSgt Reidy, USAF, 1993)

33

Power down procedures complete, SSgt Reidy mustered his personnel, secured the DPC and evacuated to the Agricultural College.

During the eruption, Pinatubo's ash mixed with the typhoon's downpour and turned into falling concrete, violently pummeling the now-deserted air base. From 1:30 p.m. Saturday onward, fifteen hours of violent explosions ripped the volcano. Its summit collapsed into the rising, fiery magma and was blown back into the air. Later, when the mountain had subsided, scientists judged that they had just witnessed the most powerful volcanic eruption of this century. (Grier, 1992, p. 59)

## J. RECOVERY PHASE

U. S. personnel weren't gone for long. A vanguard security force was back on the base by Sunday morning, June 16, barely twelve hours after the last man had left. They returned to something far different from what they had left.

A lush tropical landscape had been turned into a moonscape. Everything was buried under four to eight inches of rapidly hardening ash. Trees resembled big upright pencils, lacking branches or leaves. The weight of the ash and the undermining force of the earth tremors had destroyed 111 buildings, including a gym, seven warehouses, part of the powerplant, and all of the hardened aircraft shelters.

The bookstore and the NCO club had been flattened by rapid mud flows called lahars. Superhot pyroclastic flow from the volcano had come close to the base, traveling down a riverbed to within a few hundred yards of base housing. (Grier, 1992, p. 59)

After the eruption had subsided, SSgt Reidy and another airman traveled by truck to the Naval Air Station at Cubi Point. At Cubi they, along with the backup tapes boarded an aircraft that would transport them to Kadena AFB, Clark's alternate processing site.

## 1. Resuming Operations

Upon SSgt Reidy's return to Clark from Kadena AFB, he and his DPC crew began the arduous task of resuming operations to support the 1,500 Air Force and civilian personnel left at Clark. Although covered with six inches of cement-like ash, the facility was otherwise undamaged. SSgt Reidy stated:

> It was surprising to come back a few days after--the place looked like the surface of the moon. (Interview, SSgt Reidy, USAF, 1993)

On reentering the mainframe computer room, the DPC staff was surprised to discover the mainframe operating as they had left it. The UPS had functioned perfectly, supplying power to the mainframe and environmental control units throughout the eruption and ash fall that followed.

During this period, the DPC operated the mainframe computer, a communications front-end processor, three personal computers (PC), two Zenith 248 model computers that served as terminals and two line printers.

Normal on-site processing functions (Payroll, Personnel and Accounting/Finance data transactions) were resumed within one week following the eruption.

Accessing the few remaining telephone lines between Cubi Point and Clark, the DPC also supplied processing support for Air Force aircraft flying relief missions from NAS Cubi Point. Connected by modem with computer terminals in Cubi, the DPC processed Aircraft Maintenance and Administrative data for transient aircraft and their crews.

Initial communications with Clark's alternate site at Kadena AFB were less than satisfactory.

SSgt Reidy:

> Data processing personnel at Kadena attempted to transfer files to Clark using the Defense Data Network (DDN), but the most important files (Personnel, Accounting and Finance, Aircraft Maintenance) were too large for existing data transfer protocols. Eventually, Kadena communicators set up a data base schema that would accept the large size of our most important files. (Interview, SSgt Reidy, USAF, 1993)

## a. Subic Processing Operations

Arriving at Subic Bay, MSgt Licci was tasked to provide temporary Accounting/Finance and Personnel data support for the evacuees. Two Navy computer terminals and peripheral devices were allocated for Air Force use. MSgt Licci unsuccessfully attempted to obtain an Air Force mobile satellite communications van to uplink via satellite with Kadena AFB. MSgt Licci said:

> I wanted to get a mobile satellite-capable comm van so we could establish data circuits from Subic to Kadena, and the States, but had no luck. The only way I could get any service to the terminals was to get a land-line link between Subic and Clark, and use the SATCOM facility at Clark to link to Denver, Colorado for Accounting/Finance. (Interview, MSgt Licci, USAF, 1993)

Licci also helped Personnel users link their terminals with Air Force Personnel headquarters at Randolph AFB, Texas.

After Black Saturday (June 15) and the disabling of the Clark SATCOM facility, automated processing of any type became impossible. On Sunday, June 16, MSgt Licci and his family, along with an estimated 22,000 evacuees, boarded Navy ships enroute to the United States.

## K.  RELOCATION PHASE

Back at Clark, life was not returning to normal.  As damage-control teams set to work, they discovered a shortage of a key item--shovels for clearing ash from roofs, sidewalks and roads.  Officials placed a rush order for 200 snow shovels from Elmendorf AFB, Alaska.  Clark, meanwhile, turned one of its damaged workshops into a shovel factory, churning out 800 shovels in a few weeks.

Ash falls and tremors continued to hit the area.  Many members of the mission-essential crew spent the nights in their cars instead of buildings, which were in danger of collapsing.

Three hundred Filipino contract workers were hired to clean up, but much of their time was spent packing the household goods of evacuees.

Base security continued to be a concern.  SMSgt Futch, a member of the mission-essential team said:

> Looting was a problem, though it was not being done on the scale people have been led to believe.  (Grier, 1992, p. 60)

After the evacuation began, the base experienced ninety-six break-ins in government buildings and another 200 in the base housing area.  (Grier, 1992, p. 60)

The Clark Data Processing Center was located well inside the base perimeter and was not an easy target for thieves. For whatever reason, Filipino looters had bypassed the facility.

During this period, SSgt Reidy and the DPC staff continued their data processing activities, while assuming the additional tasking requirements of Civil Engineering personnel who had arrived to assess post-eruption damage. The DPC assisted engineers by transcribing to magnetic tape reports of monetary damage, repair costs and other reports. Using a temporary microwave communications link set up after the eruption, DPC personnel transmitted this data to Kadena AFB for further transfer to the United States.

Once the decision to abandon Clark AFB was made, DPC personnel were among the last to leave. The Sperry mainframe computer, peripherals, magnetic tapes and other supplies was shipped to Andersen AFB, Guam. The Center provided limited administrative computer support until November 26, 1991, when they closed and locked the facility for the last time.

## L. CONCLUSIONS

Until April 2, 1991, the Clark AFB Data Processing Center, along with the rest of the personnel stationed at the air base, had not considered volcanoes a threat. It was a reasonable assumption, as Pinatubo had not shown any signs of volcanic activity for over 200 years.

A lack of existing guidance led to the formulation and use of imaginative methods to cope with Mt. Pinatubo's eruption.

The Volcano Plan was a masterpiece of innovation and common sense. Devised by an experienced Air Force computer technician, MSgt Joseph Licci, the Plan maximized advantages the Center possessed prior to the eruption: an experienced staff, a tested backup routine and alternate processing sites capable of assuming Clark's processing requirements.

Although the Plan was technically and operationally sound, it nearly ended in failure with the cancellation of alternate site processing operations by a senior DPC official.

Communications deficiencies plagued the recovery effort. Some were unavoidable, but problems could have been reduced. Practice exercises using mobile satellite communications vans to link with alternate sites would have familiarized DPC personnel with this critical procedure. Had they done so, the automated data processing effort would have been more productive.

Disregarding the difficulties encountered, the DPC's recovery from the "eruption of the century" was successful. No lives were lost and the facility resumed a satisfactory level of operations in a minimum amount of time. This success was largely due to the professionalism and courage of SSgt Reidy and the essential personnel left behind to operate the Clark DPC. Adapting to uncertainty, danger and extreme adversity, they preserved vital data files, activated alternate site operations and resumed processing in a most efficient manner.

If the Pinatubo disaster had happened elsewhere, the Air Force perhaps would have begun shaping its long-range recovery plans immediately, but Clark's future had been in doubt for years by the time the volcano blew. Coming in the middle of basing rights negotiations, the explosion only hastened what may have been inevitable. (Grier, 1992, p. 60)

## IV.  HOMESTEAD AIR FORCE BASE INCIDENT

### A.  OVERVIEW

This segment examines the contingency planning and disaster recovery efforts of Homestead Air Force Base (AFB), Florida and its data processing facility following a major natural disaster.

Homestead AFB, an Air Force installation located ten miles southwest of Miami, Florida bore the brunt of Hurricane Andrew, a destructive storm that laid waste to much of southern Florida and Louisiana in August 1992.

During this period, base and computer center contingency plans were activated and used; these plans can therefore be analyzed as to their usefulness in an actual disaster setting.

Also studied are the storm's effects on the surrounding communities, local citizens, and commercial computer information systems.

### B.  A HURRICANE IS BORN

Hurricane Andrew began on or about August 13, 1992 as a patch of thunderstorms over western Africa, moving out over the Atlantic Ocean as a rainy low-pressure wave.  U. S. National Hurricane Center satellites track 60 or 70 of these waves each hurricane season (June through November).  This

disturbance seemed unusually strong. By Monday, August 17, it had intensified into a tropical storm, developing a central circulation but not yet the clear "eye" that characterizes a strong hurricane.

Then it encountered meteorologic problems. A well-developed eye resembles a chimney. At its edges warm, moist air near the ocean surface spirals up to altitudes where the moisture condenses and releases its heat energy. But high-level wind shear over the Atlantic tugged at Andrew's central chimney and kept it from staying well aligned. Weak and disorganized, Andrew began to veer north, toward the open ocean. (Gore, 1993, p. 14)

Then, two days and a thousand miles off Florida--the wind shear diminished. Also, a high pressure zone to the north grew stronger, pushing Andrew back westward. Still, most of South Florida went to bed anticipating a relaxing weekend.

Not Bryan Norcross, a TV weatherman at Miami's WTVJ who had long been trying to warn his fellow Floridians to prepare for "the big one"--the major hurricane that would one day strike.

"I didn't like the looks of this storm," recalls
Norcross. "I knew that soon someone within the sound of my
voice was going to have a hurricane--and maybe a bad one."
(Gore, 1993, p. 14)

When Norcross returned to work Saturday, Andrew's winds
had reached hurricane strength--74 miles an hour. Norcross
recalls thinking that day that it might not be so bad for
South Florida to have a hundred-mile-an-hour storm to shake
resident's complacency about hurricane danger. But on
Sunday, as Andrew's winds grew to 150 miles an hour, he
realized that thousands of lives could be lost.

As Hurricane Andrew bore down and highways out of South
Florida clogged and shelters filled, countless viewers heard
Norcross' urgent warnings: "It's absolutely for sure. No
question about it. It's going to happen tonight." (Gore,
1993, p. 14)

1. A "Zone of Devastation"

Andrew transformed south Dade County, Florida--home
to 350,000 people--into a zone of devastation larger than
the city of Chicago. Virtually every building was ravaged;
80,000 dwellings were demolished or damaged too severely to
live in.

Hurricane Andrew--in its toll of destruction and
economic loss--was the most devastating natural disaster
ever to strike the United States. In Florida it took a low
count of 43 lives, because residents heeded evacuation and
emergency warnings. It also destroyed perhaps 30 billion
dollars' worth of property. (Gore, 1993, p. 15)

National Hurricane Center (NHC) meteorologists
estimate sustained winds of 145 miles an hour with gusts of
175. They concede that winds may have approached 200 miles
an hour in places.

It was clear in the Miami metropolitan area that a
hurricane had passed through. Traffic lights were out.
Trees were uprooted. The headquarters building of Burger
King, the fast-food giant, took a direct hit. Floor after
floor of windows had been blown out. Desks, computer
screens, and file cabinets were flipped over and smashed.
Ceilings and walls were ripped away, exposing ducts and
pipes. Some equipment was found two miles away. (Gore,
1993, p. 20)

Looters helped themselves to resident's shattered homes. Sporadic acts of violence erupted as homeowners defended what few possessions they had left. Volunteer worker Jo Ann McGinnis, a resident of Homestead, Florida, described her community's ordeal:

> ...people were crazy, breaking into stores, stealing and grabbing.... (Gore, 1993, p. 20)

Many people shared the nightmare of Andrew. Down U. S. Highway 1 in Cutler Ridge, Florida (a community southwest of Miami), security guard C. C. Jordan stands alone on a jumble of concrete slabs. Before Andrew arrived these slabs had formed the walls of a warehouse. "I'm lucky to be alive," he says. Under one huge slab lies a crushed truck. "I was sitting in that." (just before the warehouse collapsed) (Gore, 1993, p. 23)

## 2. Effects on Commercial Information Systems

Thanks to timely and accurate weather forecasting, many data center managers in the lower Southern states were prepared for Hurricane Andrew. "Most of the customers we were able to contact had backed up their data and were in pretty good shape, but south Dade County, Homestead, those areas--you can forget it. The last thing they're thinking about is their computer systems," said Carl McKinley, director of customer service at Maynard Electronics, a corporation that makes data backup systems. (Anthes, 1992, p. 6)

For more than one south Florida information systems manager, the first days after the storm were spent making sure employees still had homes to return to when the work day was over. Lewis Temares, Chief Information Officer at the University of Miami said, "I've got 12 people homeless on my staff, and there are still 22 people I haven't even heard from." (McPartlin, 1992, p. 12)

"This is the largest single disaster to affect computer facilities," said Teri Schrieder, chief executive officer at Contingency Planning Research, Inc., a disaster recovery consulting firm based in Jericho, New York.

According to Schrieder, by the last week of August 1992, 39 major companies had moved to backup processing sites provided by disaster recovery firms.

Some smaller firms did not arrange for a backup processing site and considered themselves lucky they did not need one. Jon Paul Olivier, director of computer operations at Gulf South Engineers, Inc., in Houma, Louisiana said that he wrapped his Digital Equipment Corporation Micro/VAX II and his personal computers in plastic and moved them to higher ground before the storm. (Anthes, 1992, p. 6)

## C. HOMESTEAD AIR FORCE BASE DEVASTATED

### 1. In the Path of the Storm

After watching Hurricane Andrew grow and pick up speed over four days, Air Force Colonel Steve Plummer, commander of Homestead's 31st Fighter Wing, put the base's disaster response plan into action early August 23, 1992.

"The plan is very specific on when we should evacuate," Plummer said. "When the storm reaches Category III force (sustained wind velocity 111 to 130 m.p.h.), the plan dictates that we will evacuate all personnel except those I deem are absolutely essential. I ordered the evacuation about 24 hours out. The people I selected to remain behind were from the disciplines I thought I might need immediately after the storm, like external power production people, firefighters and security police."

Plummer and his team chose the base's alert facility for shelter. The hardened building, which includes sleeping quarters for aircrews and bays for alert aircraft, was the structure most likely to escape damage. For more than five hours, Plummer wondered whether he and his men would survive. "There was nothing we could do but hope the shelter we were in wouldn't come apart. It was a very helpless feeling." (Gillert, 1992, p. 12)

## 2. Andrew's Heroes

In the midst of Andrew's fury an Air Force
firefighter, SSgt Steve Wilensky volunteered to climb to the
top of the shelter and close a steel hatch on the roof. The
howling winds had blown the hatch open, creating a vacuum
that threatened to collapse the building. "We tethered him
to the ladder and held on to his legs, but he still could
have been seriously injured or killed," Plummer said. "But
we had to get that door closed or the building would not
have made it." (Gillert, 1992, p. 12)

Wilensky said what he most remembers about the
hurricane were the feelings of complete isolation and the
noise. "By 3 (p.m. August 23) most of the people had gone
and we started securing the base," he said. "It started
getting dark about 8, and we tried to get some sleep. About
four o'clock (in the morning) we were woken up by the wind.
It was really starting to come at us. We started hearing
slamming and banging. Some of the (ground-level) doors blew
open, and we tried to secure them. But they were off their
tracks and couldn't be closed."

The wind sucked at some of the interior doors, and the men struggled mightily to keep them closed. Wilensky recounted: "The noise was terrible. It sounded like a freight train, like kids jumping around on the roof. We saw cars moved several feet by the wind." (Gillert, 1992, p. 13)

The team received temporary respite when the hurricane's eye passed through. For a while after the storm resumed, the shelter was quiet. Then the roof started giving in. Wilensky said he wasn't sure at that point that they would make it out alive. But the storm finally passed, and they escaped the refuge that threatened to become their grave.

After the hurricane wrecked Homestead Air Force Base (AFB) on August 24, 1992, Colonel Plummer's first priority was to make sure nobody was killed. Nobody was. The next step: "to establish and maintain an environment where people can work and live without fear of disease or injury," Plummer said. (Gillert, 1992, p. 12)

### 3. The Aftermath

"Homestead Air Force Base, home of Air Combat Command's 31st Fighter Wing, no longer exists" was among the first reports to air on television after the deadly storm ripped through the base during the predawn hours of August 24, 1992.

The storm, touted as the worst natural disaster in U. S. history, hammered the base with winds approaching 200 miles an hour, leaving an unimaginable trail of devastation and indefinitely shutting down base operations. (Haggerty, 1992, p. 2)

Most base facilities were damaged. The hurricane tore roofing off all but a few of the 1,613 base houses. Two 31st Fighter Wing F-16s (fighter jets), which couldn't be evacuated before the storm, were blown from their hangars and dismantled by the winds.

Those who returned to the base were stunned by the aftermath of the killer hurricane. "If we tried to bomb this place, we couldn't have done it this well. It's total and absolute devastation," said Air Force MSgt Dennis Doome, a member of a Reserve unit assigned to the base. (Haggerty, 1992, p. 5)

## D. HOMESTEAD AFB COMPUTER CENTER--EVACUATION

For Captain Chris Moore, Deputy Commander of the 31st Communications Squadron and (now retired) MSgt Jim Knueppel, Superintendent of Homestead's Base Communications and Computer Center (BCCC), the oncoming hurricane signaled the beginning of a period of frenzied activity. When ordered by his squadron commander, Moore, a seven-year Air Force veteran activated the BCCC's Emergency Action Procedures (EAP). (Interview, Captain Moore, USAF, 1993)

## 1. Emergency Action Procedures

Complying with Air Force 700 Series Regulations, Homestead BCCC Emergency Action Procedures training had been accomplished and documented on a quarterly basis. Prior to Andrew's arrival, the EAP had been updated to reflect the Regionalization of the facility.

The Regionalization concept (described at length in a subsequent section) was the outcome of the U. S. Congress' Defense Management Report Decision (DMRD) 924. As a budgetary/management measure, DMRD 924 would consolidate smaller, base-level data centers such as Homestead AFB with larger computer facilities to form Regional Processing Centers (RPC). (Interview, LtCol Compton, USAF, 1993)

Under this concept, called Distributed Communications Processing (DPC), mainframe computers would be concentrated in the RPC while functional user input terminals and printers remained at the base. Under DMRD 924, sixty-six active Air Force bases are to be regionalized to five geographically-located RPCs by mid-1995.

Prior to Hurricane Andrew, most of the BCCC's hardware, data bases and tape library had been moved to Gunter AFB, Alabama, Homestead's designated RPC. Communications and cryptologic equipment, consoles and user terminals remained at Homestead. Connectivity between Gunter and Homestead was established by means of the Air Force Network (AFNET). (Interview, CMSgt Reed, 1993)

52

The EAP was considerably updated; an unexpected by-product of regionalization. The plan was reviewed and modified, removing procedures pertaining to the missing equipment and processing functions.

Risk assessments were conducted quarterly. After the assessment was complete, the EAP was amended to reflect new threats to the facility. Due to the air base's coastal location and vulnerability to tropical storms, hurricanes constituted a very real threat and represented a major portion of BCCC contingency planning.

### 2. Personnel Move to Safety

With the exception of MSgt Knueppel and two unmarried airmen, Captain Moore relieved all other BCCC personnel from duty and accompanied them to shelter. Knueppel and the two airmen would remain to secure the facility in accordance with the EAPs. (Interview, Captain Moore, USAF. 1993)

### 3. Preparing for Andrew

Following EAP guidelines, MSgt Knueppel and his small crew readied the BCCC for the onset of Hurricane Andrew. When asked about specific actions that the crew were to perform prior to a disaster, Moore stated that:

Without the EAP's in front of me (all copies were destroyed), I cannot give you the exact order in which they carried them out. Our primary concern was the storing and securing of classified (materials) to include classified messages, plans, documents and manuals. (Interview, Captain Moore, USAF, 1993)

Once the BCCC's classified materials were secured, the following procedures were accomplished:

- High-priced computer components were stored in Vidmar (watertight) cabinets.

- All data equipment was powered down (modems, modem nests and the console that monitored the base Data Network).

- To protect against water damage, equipment was covered with specially-made plastic covers.

- Squadron members made telephone contact with the BCCC, stating their location and intentions. Evacuation and safety procedures were emphasized. (Contact was made with approximately 99% of squadron personnel)

BCCC communications and cryptologic equipment were to remain energized regardless of the situation. It remained so until emergency messages were sent to the Gunter RPC and MacDill AFB (located in Tampa, Florida--far from the storm's center) advising them of the BCCC's situation and intentions. Following that transmission, by order of the squadron commander, all remaining equipment was deactivated.

Disaster preparedness training conducted by the BCCC paid big dividends in performance. As a result of their quarterly EAP training, the three airmen:

> ...needed very little guidance on what to do. In fact, not only did they send required (emergency) messages to Gunter AFB, they also requested that Minimize conditions be imposed for Homestead AFB. This action eliminated higher headquarters from getting swamped with messages destined for Homestead. (Interview, Captain Moore, USAF, 1993)

When all the pre-disaster procedures were completed, the crew secured the BCCC and moved to shelter. It would be days until they could return. (Interview, Captain Moore, USAF, 1993)

## E. RECOVERY

In Andrew's wake, ordinary people did exceptional things to bring aid to storm victims. At Homestead AFB, food, toiletries, water and clothing arrived daily, donated by communities around the United States and flown in by military aircraft. The base wasn't established as a distribution center, however, and pallets began piling up. The solution: find a way to get the supplies to people in need. After borrowing a few of the base's two-and-a-half ton capacity trucks, a group of airmen began distributing supplies to the hardest hit areas north of Homestead: Cutler Ridge, Perrine, Goulds and Richmond Heights.

"These people really need help," an airman said.  "This is worse than what you see on the news.  They need it all--food, water, the works."

Over a span of several days, relief personnel managed, with the help of off-duty volunteers from the base, to deliver over 360,000 pounds of relief supplies.

An emergency response team also assisted people at Homestead.  Five days after the storm, the team helped the returning population with personnel concerns, pay issues, Air Force Aid Society assistance and claims processing. (Haggerty, 1992, p. 6)

With nearly 25,000 troops working in the area, tent cities went up all around Dade County.  The Army's 82nd Airborne Division from Fort Bragg found itself in a different role: patrolling neighborhoods for looters, serving hot meals, pulling wet carpets out of houses and providing medical care for victims.  "God sent us angels in red berets," Andrea Martinez of Cutler Ridge said.  "I feel safer knowing they're here."

The runway at Homestead was busy.  In one day, the base received 105 flights and 700 tons of cargo.  "Not only is our airlift support of Hurricane Andrew the largest operation Air Mobility Command has ever undertaken, it is the biggest and fastest domestic relief operation effort ever done by air in the history of the Air Force," said General Ronald R. Fogelman, commander-in-chief of the U. S.

Transportation Command. Fogelman stated that the tons of cargo moved by air into Florida over the first 10 days following the storm nearly equaled the amount airlifted to the Persian Gulf in the first ten days of Operation Desert Shield. (Haggerty, 1992, p. 7)

### 1. Information Systems Aid Civilian Recovery Effort

The Federal Emergency Management Agency (FEMA) had established a computer network spanning four disaster assistance centers in south Florida. The network could support up to 200 users and process requests for disaster relief. The FEMA Network--actually several local-area networks connected by T1 (1.5 megabit per second capacity) lines--consisted of server computers, user terminals and a fault-tolerant storage management system providing continuous backup of data files.

The American Red Cross had also deployed a 12-node local area network and software developed to perform damage assessment and account for Red Cross staff, supplies, vehicles and expenses. The Red Cross and FEMA networks were compatible, facilitating data sharing between the two relief groups.

## 2.   Homestead BCCC Disaster Recovery

Despite extensive damage to the Homestead BCCC, disaster recovery did not occur in the classic sense; Homestead had migrated most of its computer operations to the Gunter RPC months before the storm.

Via a dedicated communications link, Homestead's data was backed up and stored at the Gunter RPC.   Partial file transfers were accomplished daily; complete backups were performed and stored each week.   As a result, no Homestead BCCC data was lost as a result of the hurricane.

Regionalization of Homestead's computer facility had eliminated most of the common disaster recovery steps: up-to-date off-site storage of programs and data bases, current alternate site support agreements and experienced technicians deploying with portable sets of operating instructions and data backups to alternate processing sites.

"Recovery," therefore, was limited to reestablishing data communications and input/output capability to the bases where Homestead's functional users had dispersed. (Interview, CMSgt Reed, USAF, 1993)

### a. BCCC Personnel Reassigned

Andrew had destroyed the BCCC's ability to function.   Without a facility to operate from, most of Homestead's functional users were reassigned to Gunter AFB, MacDill AFB and Patrick AFB, Florida.

At MacDill and Patrick Air Force Bases, Homestead personnel would restore only those processing functions not yet performed by the Gunter RPC (Accounting/Finance and Civilian Pay). Connectivity was obtained with the Gunter RPC via the Air Force Network (AFNET), a 56 kilobits per second (KBPS) data communications link.

On arrival at Gunter, users were assigned passwords, user identification, terminals and data base access privileges. Connectivity was established with other facilities via the AFNET. Homestead data processors quickly went back to work, quickly resuming normal processing levels.

### 3. Gunter AFB Regional Processing Center

The Gunter RPC, the first of five Regional Processing Centers to be established throughout the United States, played a major role in Homestead's recovery effort.

Located at the Gunter Annex, Maxwell AFB, Montgomery, Alabama, the RPC provides standard base-level computer (SBLC) data processing support to ten Air Force bases and twelve Air National Guard bases located across the United States' southern region.

The RPC uses both voice and data communications systems, consisting of local and long-haul (AFNET) networks to provide reliable, high-quality circuit connectivity to its supported bases.

Gunter RPC personnel operate ten UNISYS mainframe
computers, monitor the operation of robotic magnetic tape
silos, support over 200 databases, manage over 50,000
magnetic cartridge tapes and perform a host of other
processing tasks.  The RPC is segmented into five functional
divisions, described as follows:

- Operations Division--Provides 24 hour, 7 day a week
  operational support to base-level centers.  Equipped
  with an array of UNISYS 2200 Series processors and a
  robotic magnetic cartridge tape library system. Also
  furnishes continuous Automated Digital Network (AUTODIN)
  data message traffic support through the Host Autodin
  Message Processing System.  Division personnel perform
  system recoveries during planned/unplanned system
  outages.

- Systems Management Division--Supplies system monitors
  who act as the primary focal point for base level
  customers, ensuring prompt responsiveness to customer
  needs.  Each monitor supports three installations on a
  full-time basis.  Monitors verify receipt of input data
  from ten Air Force and twelve Air National Guard bases
  and load new software releases for assigned systems.

- Database Management Division--Responsible for
  configuration management of ten UNISYS mainframe
  computers and eight magnetic tape silos.  The Division
  manages the largest distributed processor network in the
  Air Force, providing data connectivity for over 20,000
  RPC customers throughout the southeastern United States.

- Network Management Division--Acts as the primary focal
  point for communications-related issues for the RPC.
  Network Management oversees the 56 KBPS high-speed data
  network connecting the RPC to each supported base and
  monitors RPC local area networks.  Acts as configuration
  manager for TELCON communications software; serves as
  focal point for AFNET service requests.

- Plans and Requirements Division--Responsible for
  hardware management, fiscal year budgeting and customer
  support.  Accountable for over $16 million in equipment.
  Gauges customer satisfaction by using telephone and
  written surveys.  (Interview, J. Buckner, 1993)

60

The Gunter Regional Processing Center is capable of accepting the computer operations of inoperative base-level sites. Designed to 125% of normal data processing capacity, the RPC has sufficient processing power to assume a damaged/destroyed remote site's computerized tasking, as was done with Homestead AFB. All future RPC's will eventually possess this enhanced capability. (Interview, J. Buckner, 1993)

## F.  RELOCATION

When asked about the feasibility of rebuilding Homestead AFB the commander of Air Combat Command, Air Force General John M. Loh said that the first step will be to assess the damage, estimated by the Pentagon to approach $480 million. "Right now, we're making an assessment of what it would take to rebuild Homestead. It will be costly and take a long period of time," Loh stated. (Barela, 1993, p.8)

After the hurricane, entire Homestead-based aircraft squadrons and support units were reassigned to other duty stations. By September 2, 1992 over two thousand officers and airmen had been transferred.

The reassignments followed an announcement by then-President Bush on 1 September that the federal government would rebuild the base, subject to Congressional approval.

The Homestead BCCC still has not fully recovered from Hurricane Andrew. In an interview with Captain Moore in March 1993, Moore described the hurricane's effect on the base as:

> Unbelievable. As a Florida native, I had gone through three storms, but I had never seen anything like it (damage). Two-thirds of the BCCC's roof was gone. Everything inside was wet, and there were several inches of water under the raised floor in the equipment room. Just incredible. (Interview, Captain Moore, USAF, 1993)

Moore, now commanding the 31st Communications Squadron, stated that an Air Force mobile data processing center was to relocate to Homestead after the storm, but was delayed and eventually cancelled.

The BCCC and the mobile center were victims of several overriding factors: the RPC's assumption of Homestead's data processing requirements, the rapidly diminishing number of Homestead-based personnel and uncertainty clouding the base's future.

## G. ADVANTAGES/LESSONS LEARNED

From Homestead AFB's experiences, DOD Information managers can obtain useful information that should prove useful in their contingency planning efforts.

Advantages, lessons learned and recommendations are listed below:

- The presence and cooperation of the Gunter-based cadre of experts who promptly absorbed Homestead's users into their organization, opened communications with remote sites and rearranged RPC processor tasking to perform Homestead's critical tasks with a minimum of delay.

- The Gunter RPC was specifically designed with excess capacity to assume the workload of a damaged/destroyed facility. This capability was a key factor in the efficient resumption of Homestead data processing operations.

- MacDill and Patrick AFB's cooperation in assuming Homestead's data processing functions that were not yet being performed by the RPC. For example, Homestead Accounting/Finance functional users migrated to MacDill, set up operations and quickly resumed work.

- The Regionalization concept, in conjunction with the automated file transfer routine instituted by the Gunter RPC, permitted the efficient resumption of Homestead's critical processing functions. Had Homestead not transferred the bulk of its hardware and data files to Gunter prior to the hurricane, all the classic disaster recovery steps--with associated delays--would have been present.

- Disaster preparedness training pays off. The three airmen that secured the BCCC knew their responsibilities and carried them out without hesitation. This noteworthy performance under stressful conditions came from confidence gained in rehearsals under realistic practice conditions.

- Avoiding bureaucratic "snarls," communications circuits were quickly restored and hastened resumption of Homestead's critical data processing functions-- primarily Accounting/Finance operations from MacDill AFB.

- Captain Moore recommends that, with regionalization taking place throughout the Air Force, "quick disconnects" should be mounted on the smaller, more portable data equipment found in base-level centers. In a minimum of time, equipment could be disconnected, loaded in trucks and evacuated. He further recommends that each user be trained in detaching several pieces of dissimilar equipment for removal in emergencies.

## H. DISADVANTAGES

Homestead BCCC's existing Emergency Action Procedures proved to be effective during Hurricane Andrew. No lives were lost, Homestead data was saved and processing resumed. However, there were several disadvantages noted and adverse lessons learned by the Air Force and Department of Defense (DOD) personnel who participated in the BCCC recovery effort. They are:

- The plastic covers that shielded the BCCC's computers and other equipment retained moisture to such an extent that extensive corrosion developed within the covered equipment. Due to the destroyed roof and damage to the BCCC's environmental control units (air-conditioners and humidifiers) there was no way to adequately dry out the facility. Trapped moisture possibly caused as much damage as rain would have on uncovered equipment.

- Captain Moore stated that the EAPs should have been activated two days in advance of the hurricane, to include the total evacuation of personnel. However, Moore added that, due to Andrew's total devastation of the base, leaving a week earlier would have made little difference. In this instance, the EAPs saved lives but were unable to save the data facility.

- The loss of an RPC with all of its centralized processing capability would be a crippling blow to the base-level centers. RPCs will ultimately act as each other's alternate sites, but until they are completed immense difficulties would arise should an RPC be destroyed.

# I. EPILOGUE

Gore wrote of but one advantage to come from the devastation caused by Hurricane Andrew. An excerpt from his magazine article is transcribed below:

Andrew has had this positive impact: it has brought South Florida's residents--a diverse, often bizarre and troublesome lot--closer together. "Homestead (Florida) was blown into the 21st century," says city parks director Paul Burleson. "We'll be the newest city in the country." But beneath the courageous statements lurks a deeper feeling, one that was scrawled across the only remaining wall of a crumbled home. It says, "Damn you, Andrew." (Gore, 1993, p. 37)

## V. DFAS/DITSO KANSAS CITY ORGANIZATION AND BACKGROUND

### A. ORGANIZATION

The U. S. Marine Corps Finance Center, and the computer center that supports the Finance Center's activities, is located in Kansas City, Missouri. As part of a Congressionally-mandated consolidation scheme, the financial portion of the organization was recently reorganized and renamed, and is now part of the Defense Finance Accounting Service, or DFAS. The computer center also was reorganized, and was integrated into the Defense Information Technology Service Organization, or DITSO. These organizations will be referred to as DFAS-KC and DITSO-KC.

#### 1. Command Structures

Although they occupy the same building, DFAS-KC and DITSO-KC are separate organizations. Each has its own chain of command and reporting responsibilities. Each has a director with subordinate department and division heads reporting to them. The DFAS-KC table of organization in Figure 1 contains directorates for each financial activity, such as the Directorate for Vendor Payments, Directorate for Military Pay and many others. DITSO-KC organizational makeup (Figure 2) is similar to DFAS-KC.
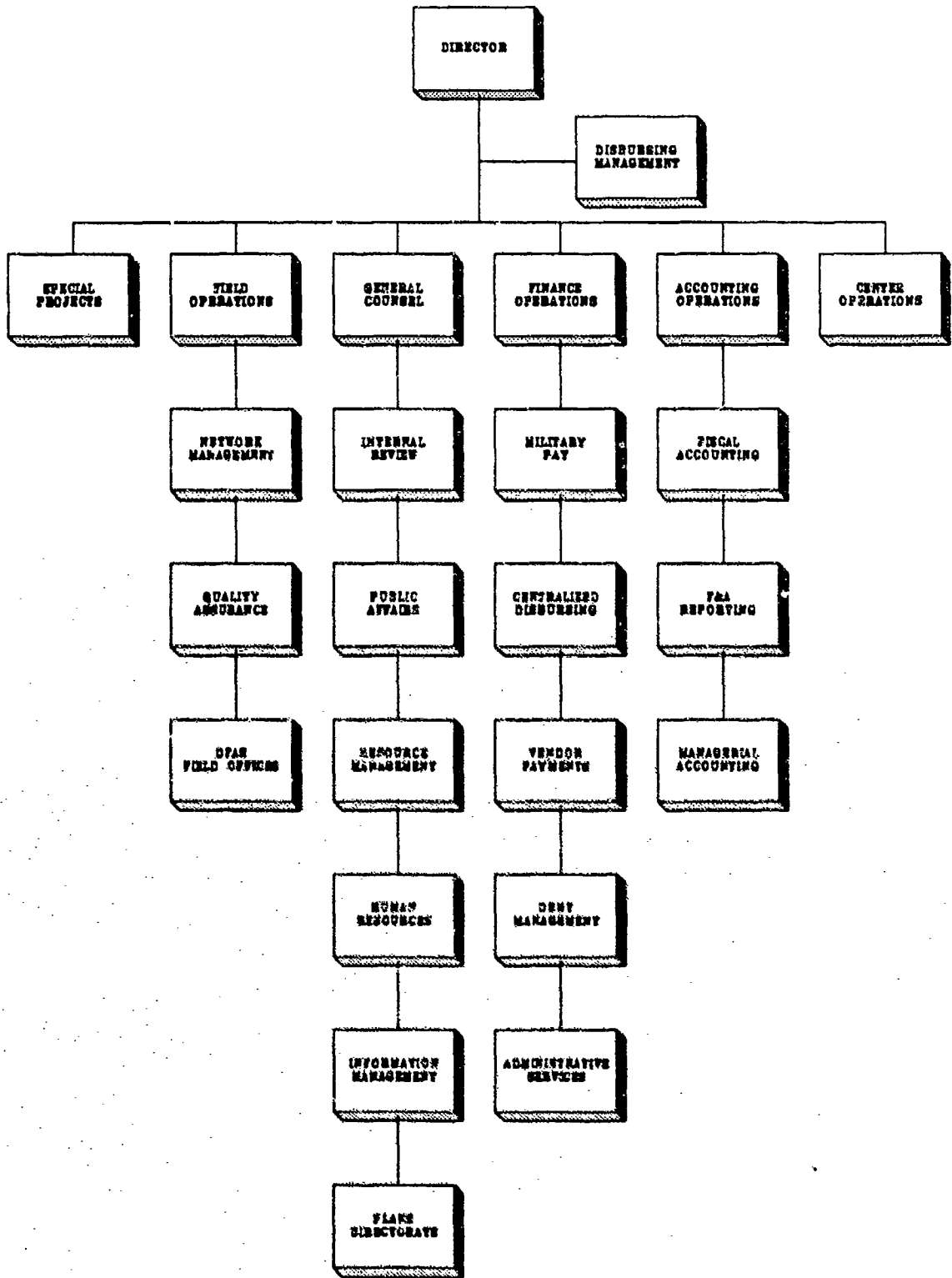
Figure 1. DFAS-KC Organization
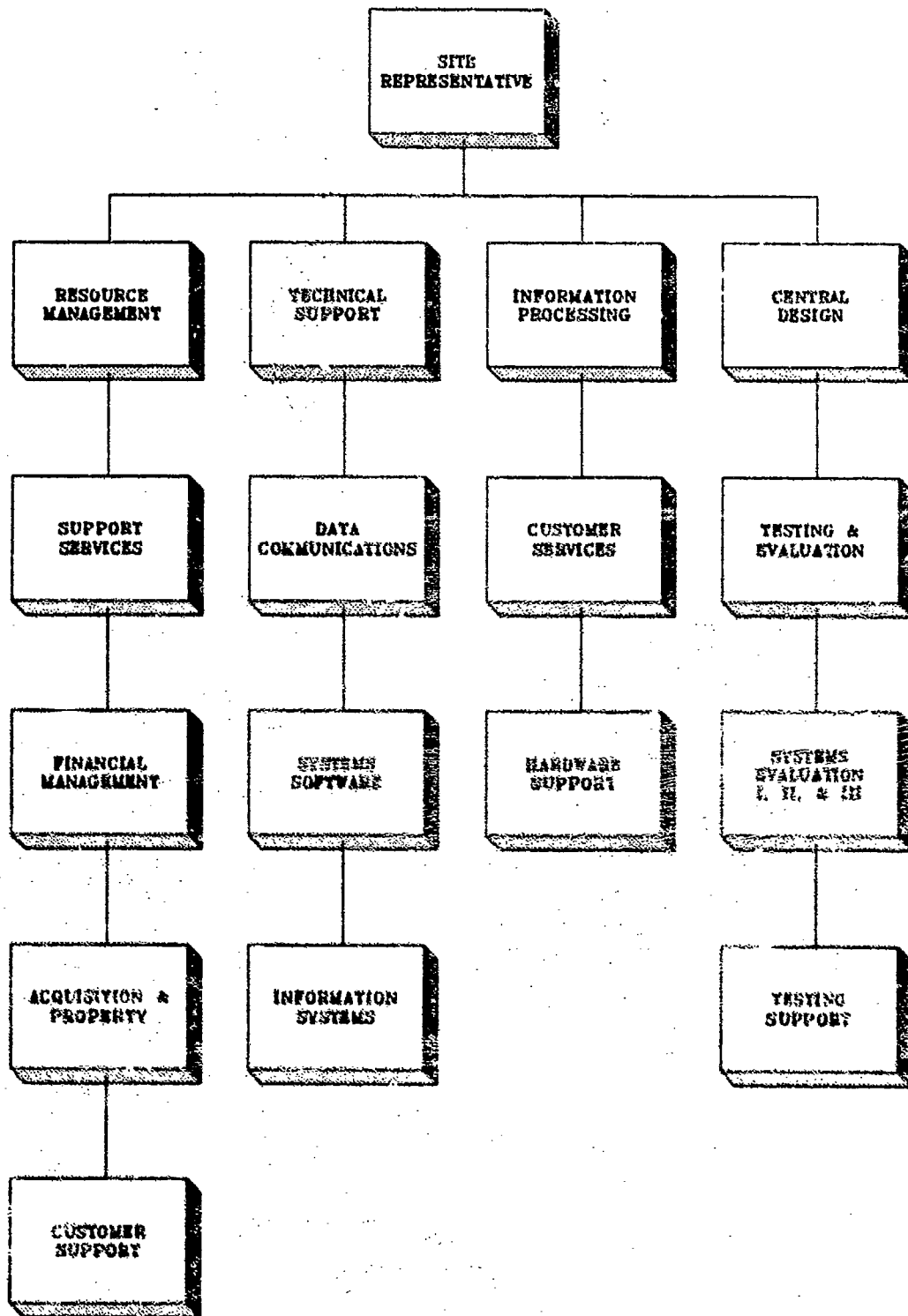
Figure 2. DITSO-KC Organization

Subordinate Divisions and Branches, headed by
Government Service (GS) rated civilians and U. S. Marine
Corps personnel, represent data processing, administrative
and support functions that make up DITSO-KC.

## B.  DFAS BACKGROUND

U. S. Marine Corps active-duty, retired and reserve
pay-related activities are the primary functions of DFAS-KC.
The accounting and administration of individual Marine pay
accounts has made great strides since the era of manually-
computed pay records maintained at the small unit level.

Marine payrolls have evolved into computerized, fully-
automated records.  Over one hundred thousand Marines
stationed around the world are served from one centralized
location.  Periodically, units electronically transmit
individual pay-related data (promotions, demotions and other
adjustments to basic pay and allowances) to Kansas City for
inclusion into individual computer files maintained on
mainframe computer accounts.  These mainframe accounts are
capable of storing hundreds of gigabytes of information.

After receipt of such data, computers make required
adjustments to specified accounts, store this data for
DFAS-KC use, and generate a personalized record of pay and
allowances for every active-duty, reserve and retired
Marine.

Printed and mailed monthly, this record is called the Leave and Earnings Statement (LES). It is a one or two page form containing each Marine's basic pay, allowances, tax data, allotments, leave accrual and balance, and other information.

# VI. DFAS/DITSO KANSAS CITY PLANNING MODEL

## A. OUTLINE

Disaster recovery (or contingency) plans can be divided into four distinct phases: planning, preparation, implementation, and recovery. (Hural, 1992, p. 5)

Using a generic contingency plan outline (Appendix) as a tool, Kansas City's plan will be partitioned into these four phases for purposes of analysis and discussion. The outline contains relevant planning categories needed to examine a contingency document and will be used to analyze the DFAS/DITSO-KC plan. (Hural, 1992, p. 15)

This phased plan outline can also serve as a reference when designing a DOD disaster recovery plan. Each phase contains unique design criteria that could assist contingency planners in the preparation of their disaster preparedness plans.

## B. PLANNING PHASE

The planning phase of a disaster recovery plan is

...used to develop the plans, programs, policies, and procedures to be put into operation to reduce the effect of a natural disaster on an organization's information system. (Hural, 1992, p. 5)

## 1. Preliminary Planning

Soon after the DFAS/DITSO reorganization, perhaps motivated by the damage caused by Hurricane Andrew, DFAS and DITSO headquarters officials called for completion of contingency planning documents by all activities, and to provide reports by 31 December 1992.  (DFAS Memorandum, 1992)

During October and November 1992, three Contingency Planning Working Group (CPWG) meetings involving DFAS/DITSO management and planning personnel from each member facility were held to discuss the state of DFAS/DITSO installation contingency plans.

Key issues discussed were:

- The need to develop detailed plans on relationships/interfaces between the two organizations related to contingency planning and programs.

- DFAS and DITSO to develop an Interservice Support Agreement (ISA) to facilitate planning.

- Formulation of a Concept of Operations for Contingency Planning to identify priorities, functions, support and technical requirements.

- DFAS requirement to provide a "strawman" concept plan as the first step in combined planning.

- Lessons learned from natural disasters.

- Plan status.

- Delay in DITSO headquarters-level planning, waiting on completion of studies by an independent contractor.

- Eventual migration to Regional Processing Centers (RPC) and its effect on individual center's contingency planning.  (DFAS Memorandum, 1992)

Plan status was discussed at length with Center planning representatives describing actions they were taking to improve and update existing plans. Several DFAS offices reported that a specialized software package designed for preparing contingency plans, DP90PLUS by Sungard Planning Solution Inc., had been purchased and loaded into PCs for use. During the 30 November 1992 CPWG meeting, a top DFAS executive expressed concern that Kansas City was not "placing sufficient resources and emphasis on contingency planning," even though this planning will "only be for several years until consolidation (of satellite centers) is complete."

The Kansas City representative reported that their existing plan, in use since 1987, had been reviewed and that the revision process had begun. DFAS-KC had also established a Crisis Coordination Center (CCC), to serve as a base of operations for the management of the recovery effort, and had started working with the DITSO-KC office. The DFAS-KC contingency plan was estimated to be complete by 15 April 1993. The DFAS-KC representative also stated that offices were being reorganized, additional people were being hired to assist with administrative details, and that contingency planning should receive more attention in the future. (DFAS Memorandum, 1992)

## 2. Plan Development

After a hesitant beginning, the effort to replace DFAS/DITSO-KC's current contingency plan, originally drafted in September 1987, was underway. In late 1992, two principal planners, one from DFAS-KC and one from the DITSO-KC organization, were assigned to rewrite and update the plan.

Faced with a 15 April 1993 plan completion deadline, principal planners began to revise their outdated plan. Several planning factors that they encountered are listed below:

### a. *Separate Plans*

Although DFAS-KC and DITSO-KC occupied the same facility and operated jointly in administering Marine Corps payrolls, principal planners were initially required to produce separate contingency plans for each organization.

While a single, integrated plan would appear to be more cost effective and easier to implement, the fact that these two organizations reported to different command structures, each with their own requirements, made separate plans unavoidable. However, the DITSO-KC principal planner attended many planning sessions and worked closely with his DFAS-KC counterpart.

Unfortunately, early in the project, the DITSO-KC planner was transferred to an extended period of additional duty unrelated to DFAS/DITSO-KC contingency planning. Faced with the loss of most of their corporate planning knowledge, DITSO-KC joined with DFAS-KC in the preparation of a single, integrated plan.

### b. DITSO Data Processing Support

In an 18 December 1992 memorandum concerning Pay System Backup and Recovery Plans, the DITSO-KC director listed the following data processing support to be provided DFAS-KC while planning for contingencies:

- Regular backup of critical DFAS files and off-site storage.

- Use of DITSO-KC's designated contingency backup processing "hot" site. However, DITSO-KC had not tested their Transportable Contingency Action Plan (TCAP), (a contingency plan that covers DITSO-KC's relocation to alternate processing sites) and could not forecast an approximate length of time before processing operations could be resumed from the "hot" site.

- Pay check generation for all Marine Corps military and civilian personnel. This process, to be accomplished within hours after relocation, would pay personnel based on amounts received during the last pay period. (DFAS Memorandum, 1992)

### c. DP90PLUS

Sungard's DP90PLUS contingency planning software was mandated for purchase by DFAS-HQ for member facilities to use in preparing their plans. DP90PLUS, a PC-based, business recovery planning product was used by DFAS-KC to automate their contingency plan development process.

75

DFAS-KC administrative personnel that used DP90PLUS initially encountered a very steep "learning curve" as the software is definitely not user friendly. Frustration mounted and requirements piled up as users struggled to learn DP90PLUS.

### 3. Critical/Vital Functions

The DITSO-KC Director had requested that processing functions be prioritized, and called for DFAS/DITSO-KC offices to identify "critical" and "vital/essential" functions and resources they would need to fulfill their mission should a disaster occur. The plan defines critical functions as:

> ...functions which, if not performed due to a disaster, would cause serious or irreparable harm to DFAS-Kansas City Center in terms of lost revenue and profits, increased operating costs, loss of customers and market share. (DFAS Draft Level III Contingency Plan, 1993, p. 195)

In the context of conventional data processing, Toigo defines critical and vital functions as:

> These functions cannot be performed unless identical capabilities are found to replace the company's damaged capabilities. Critical applications cannot be replaced by manual methods under any circumstances. Tolerance to interruption is very low, the cost of interruption very high. (Toigo, 1989, p. 35)

76

<u>Vital</u> <u>functions</u> are:

> Functions that cannot be performed by manual means or
> can be performed manually for only a very brief period
> of time. In applications classified as vital, a brief
> suspension of processing can be tolerated, but a
> considerable amount of "catching up" will be needed to
> restore data to a current or usable form. (Toigo, 1989,
> p.35)

Questionnaires were prepared and distributed among

DFAS/DITSO-KC personnel as a means of identifying "critical"

and "vital/essential" data processing functions. These

personnel were also asked to: (1) prioritize each function

as to its impact on Center operations, should a disaster-

related interruption occur; (2) specify the order in which

each function should be restored; and (3) estimate an

acceptable delay period before resumption of processing.

Examples of DFAS/DITSO-KC critical processing

functions are: Budgeting, Vendor Payment, Financial Liaison

and Lost/Damaged Records Restoration.

Each critical function, in order of priority, is

listed and described in the plan's Critical Function Report.

Members of DFAS/DITSO-KC disaster recovery teams, assigned

by name to each function, are responsible for the damage

assessment, current status, and restoration of their

assigned function following a disaster.

## 4. Plan Analysis

Despite difficulties, the DFAS-KC principal planner began revising the old plan, meeting the 28 February 1993 draft submission deadline to DFAS-HQ.

The final draft submitted to DFAS-HQ was the subject of analysis in this thesis.

## C. PREPARATION PHASE

This phase pertains to policies and procedures to be utilized in a non-emergency environment in preparation for a forecasted disaster. It also includes normal everyday procedures used to lessen the impact of an unforecasted disaster.

### 1. Purpose

The DFAS-KC Disaster Recovery Plan is designed to:

- Increase the probability of the survival of DFAS-KC Center as a business entity in the event a disaster disables the DFAS-KC facility.

- Reduce the exposure of DFAS-KC Center to financial loss as a result of the disaster. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 2)

The purpose of the Disaster Recovery Plan is to document recovery strategies, essential resources, plans and procedures necessary to meet the above objectives. This planning will:

a. Shorten elapsed time to effect a recovery.

b. Minimize costs to effect a recovery.

c. Avoid confusion and reduce exposure to error in the recovery process.

d. Avoid duplicated effort by recovery personnel. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 7)

## 2. Scope

The Disaster Recovery Plan is designed to create a state of readiness that will provide an immediate response to a disaster occurrence at 1500 E. Bannister Road (DFAS/DITSO-KC Center).

The plan addresses the scope of a disaster as a worst case scenario involving loss of the facility or loss of access to the facility, and is adaptable to lesser disasters such as loss of a single working area or piece of equipment.

Disasters are classified as:

● __Minor__--one in which the computer outage is anticipated to be about one day (i.e., in excess of one shift, but not longer than two days). Damage due to a minor disaster is not extensive. It may consist of minor damage to hardware, software, or electrical equipment from fire, water, chemicals, etc.

● __Major__--one in which the computer outage is anticipated to be from two to seven days. Damage due to a major disaster is more severe than that due to a minor disaster. For example: in the case of a major disaster, several disk drives could be permanently destroyed or severely damaged, or the computer room could suffer heavy damage but the computers (as re-configured) could be operational within the week.

- **Catastrophic**--one in which the computer outage is anticipated to be in excess of seven days. Damage due to a catastrophic disaster is severe and could involve total destruction of the Computer Center, making major replacement of equipment or significant renovation of the facility necessary. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 196)

### 3. Objectives

Plan objectives are as follows:

a. The overall recovery objective--restore critical functions within 24-48 hours of a disaster occurrence to 1500 E. Bannister Road. The Critical Functions Report contains a detailed list of essential functions.

b. Reestablish critical production processing within two business days.

c. Restore data to within one operating day of interruption, using backup tapes stored off-site. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 7)

### 4. Assumptions

The plan was based on the following assumptions:

a. Only the 1500 E. Bannister Road facility is disabled by the disruption; the backup sites are not affected.

b. The off-site storage location, where critical backup files and information are stored, is intact and accessible.

c. A full complement of qualified and trained disaster recovery personnel are available to carry out responsibilities. The recovery tasks are detailed enough for either the alternate or, if need be, back-up site personnel to effect the recovery.

d. Recovery is performed in accordance with procedures set forth in documentation.

e. Data backup and rotation procedures have been approved by management and are in place. Essential data has been identified, backed up and rotated off-site on a regular basis.

f. A telecommunications backup strategy has been approved by management; it has been successfully tested and is currently in place.

g. Plan review, maintenance and updates are scheduled on a regular basis to ensure that the plan remains ready and viable.

h. An ongoing plan awareness and training program is in place.

i. Testing of the plan is performed throughout the year. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 7)

### 5. Facility Layout

DFAS/DITSO-KC operates from a sprawling, three hundred yard square, brick and concrete building. Built by the WPA in 1942, the giant structure was originally constructed for the Pratt and Whitney Aircraft Corporation to house its aircraft engine manufacturing operation. At that time, it was the largest building in the world under one roof.

#### a. Facility Safety/Security Measures

Although the building is over 50 years old, up-to-date safety features have been installed. An overhead water sprinkling system, conforming to local/governmental fire department regulations, protects the building's occupants and contents from fire. Heat-activated sprinklers, located throughout the building's five levels, are designed so that one sprinkler head may activate to extinguish a fire without causing a chain reaction from

other sprinkler heads, thus avoiding water damage to unaffected areas.

Security is enhanced by an advanced electronic alarm system and roving security patrols. In addition, security personnel occupy control stations located throughout the facility, and respond to alarms on a 24-hour basis.

### 6. Physical Inventory

To assist in the recovery process following a disaster, a comprehensive list of an organization's assets by department, application, and service must be compiled. The physical inventory encompasses more than a list of hardware. In essence, everything must be inventoried. Items to be included in the physical inventory are:

- Internal telecommunications equipment
- Media
- Data communications
- Wiring systems and diagrams
- Vital records and documentation
- Physical environment of the facility (Hural, 1992, p. 9)

A vital segment of DFAS/DITSO-KC Center's inventory, the list of backup tapes stored off-site, is maintained by the Tape Library Team. Backup tape inventory lists are located at DFAS/DITSO-KC and at the off-site storage location.

Within each section or department, selected personnel termed "Responsible Officers" (RO), maintain detailed records that catalog and describe the equipment, machine serial numbers, wiring diagrams, users manuals and other documentation held by their workcenters.

### 7. Risk Assessment

According to Toigo, risk assessment/analysis is:

...a big term for what is essentially a straightforward application of good research and common sense. (Toigo, 1989, p. 32)

The three basic objectives of risk assessment are:

1. Identifying company assets and functions necessary for business resumption following a disaster, and prioritizing them according to time sensitivity and criticality.

2. Identifying existing threats to assets and functions.

3. Setting objectives for developing strategies to eliminate avoidable risks and minimize the impact of risks that cannot be eliminated. (Toigo, 1989, p. 32)

Risk assessment, or analysis, is the identification of risks/risk exposure, and consists of two basic operations: data collection and analysis.

### a. Data Collection and Analysis

Data collection should include comprehensive lists of computer and telecommunications hardware, and a complete inventory of applications and systems software. From this collection, system configuration diagrams can be created and annotated to show the amount of activity,

traffic, or use of each system in a typical business day, week, or month to identify critical business functions.

Organizations should then research the impact that an interruption of these critical functions would have on their productivity, and take necessary precautions to protect them. (Toigo, 1989, p. 32)

### b. DFAS/DITSO-KC Risk Assessment

A preliminary risk assessment similar to the above guidelines was accomplished by the DITSO-KC Security Department and the DITSO-KC principal planner, and identified power and hardware losses as primary risk factors. Natural disasters such as fire and flood were listed as "marginal" threats.

To determine tangible risks and threats to the facility and its operations, the DFAS-KC planner prepared questionnaires to be completed by selected employees in each department. The information received enabled the DFAS-KC planner to become more aware of an actual user's evaluation of risks present in the workplace.

Although the plan does not address methods to counter specific threats, information gained from DFAS-KC questionnaires was valuable; several potential threats to the facility and its personnel were discovered and rectified.

### c. Environmental Hazards

An interview with the DFAS/DITSO-KC facility plant manager provided information on environmental hazards that may affect DFAS/DITSO-KC. Of the various hazards discussed, floods pose the greatest danger to the Center. Seasonal heavy rainfall regularly saturates low-lying areas, or flood plains, that surround the DFAS/DITSO-KC facility. In 1962, flood waters saturated lower levels of the building, causing extensive damage.

In addition to the threat posed by flood waters, a nearby electronics plant could accidentally spill hazardous liquids used in their manufacturing process. These liquids could jeopardize the Center and its personnel.

The data processing center, located above ground on the "mezzanine" level, is not considered to be at risk from flood waters. However, water incursion within the facility could disrupt operations to the extent that alternative processing sites would have to be used.

The flood threat is being countered by the construction of a 15-foot high, $13 million dollar flood wall. Scheduled for completion in October 1993, the wall is expected to drastically reduce the potential flooding problem.

Tornadoes, a trademark of the Midwest, also threaten the building and its occupants. The facility is used as a tornado shelter by Civil Defense authorities with adequate protection for hundreds of personnel on the Sub-Basement level. Though the building is considered sturdy enough to withstand a tornado, data processing operations could be disrupted by storm damage to the local community. (DFAS/DITSO-KC Facility Manager Interview, 1992)

## 8. Backup Operations

Backup of DFAS/DITSO data is accomplished on a daily and bi-weekly basis. Irreplaceable data stored on the mainframe computer (pay accounts, unit diary information and personnel data files) is backed up daily. Also on a daily basis, local area network (LAN) data, consisting of personal computer (PC) data files, is backed up and stored at LAN server computers.

On a bi-weekly basis, the entire contents of the mainframe computer is copied to magnetic tape, sealed and moved to off-site storage. (DFAS/DITSO-KC Planners Interview, 1992)

## 9. Off·Site Storage

DFAS/DITSO-KC off-site storage is performed by a company specializing in magnetic tape storage and maintenance. Located in an refurbished former salt mine beneath suburban Kansas City, the company stores Center backup tapes until needed for use in recovery operations.

Off-site storage reference material/tape inventory data sheets, called Vault Listings, contain inventory lists of backup tapes stored off-site. These listings are kept at DFAS/DITSO-KC and at the off-site storage location for reference, when needed.

Vendor information (name, phone number, and descriptions of equipment and supplies provided) is also listed on the storage reference material/tape inventory data sheets.

Selected DFAS/DITSO-KC personnel have been authorized to travel to the off-site storage location to retrieve backup magnetic tapes, and prepare them for shipment to alternate processing sites.

For security, only one version of backup tapes is to be retrieved from off-site. Other versions are to remain off-site should transported tapes become lost or damaged in transit. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 532)

## 10. Alternate Site Processing

Should a disaster render the DFAS-KC Center unusable for operations, the plan calls for migration to selected primary and alternate "cold" or "hot" sites.

"Cold sites" are shell facilities lacking pre-positioned computers, peripherals, or supplies, whereas "hot sites" are fully functioning, operational computer centers that have the capability to perform additional data processing requirements for the period of time that the stricken facility is unusable. (DFAS/DITSO-KC Planners Interview, 1992)

## 11. Recovery Team Personnel and Training

Responding to a directive from the Management Team, Recovery Teams, composed of DFAS/DITSO-KC personnel, have been formed to restore data processing operations at the host facility or alternate sites.

### a. Recovery Team Scenarios

As described in the plan, there are two recovery team scenarios:

1. The Center is only slightly damaged, and capable of supporting data processing operations. The plan calls for recovery team mobilization and deployment within four hours after the disaster, with restoration of the mainframe system and backup networks accomplished within 16 hours.

2.  The Center is determined to be unusable.  Recovery teams are to install PCs, peripherals, telecommunications and other required equipment at the selected "cold sites" within 24 hours following the disaster.  (DFAS-KC Draft Level III Contingency Plan, 1993, p. 196-197)

Several Recovery Teams and their duties include:

- Recovery Management Team--Composed of the directors of all the major divisions within DFAS/DITSO-KC, this team reviews initial damage reports and assessments.  It estimates delays in operations and determines whether or not the disaster recovery plan should be activated.  The Management Team coordinates all Center recovery activities.

- Facility Recovery Team--Assesses physical plant damage, minimizes further losses and salvages recoverable resources.  Responsible for preparation, maintenance, and repair of backup processing facilities.

- Operations Team--Supervises alternate site computer processing activities, restores operating system software, enforces alternate processing data backup procedures, and establishes processing schedules.

- Tape Library Team--Retrieves backup data from off-site storage, performs inventory of retrieved materials, prepares tapes for shipment to the alternate processing site, and organizes the alternate site's tape library.

- Telecommunications Team--Directs voice network and telecommunications recovery activities, prepares alternate site telecommunications systems, makes required network patches, and repairs damaged communications equipment and facilities.  (DFAS-KC Draft Level III Contingency Plan, 1993, p. 210)

## 12. Hardware and System Software

Hardware and software requirements at alternate processing sites are addressed within the plan.  Listed below are hardware and software requirements for the DFAS-KC alternate processing, or "cold" site:

- FAX Machine

89

- A-B Switch, 3 each

- Laser Printer, 3 each

- Personal computers (PC), 486, 100 MB hard drives, 6 each

- Calculators, 6 each

- CXI Boards, 6 each

- LOTUS 1-2-3, version 2.4, 4 each

- Enable, version 3.0, 4 each   (DFAS Draft Level III
  Contingency Plan, 1993, p.69)

DITSO-KC's alternate processing ("hot" site), at

Camp Lejeune, North Carolina will supply operational

mainframe computers and systems software.  Also available

for use by DITSO-KC personnel are a number of PCs with

installed applications software and peripheral devices.

(Interview, MSgt Spaulding, USMC, 1993)

**13. Communications**

The plan lists data and voice communications

strategies necessary to reestablish communications between

DFAS-KC and DITSO-KC alternate processing sites.  These

strategies are:

- Data--In the event that a disaster is experienced at the
  DFAS/DITSO-KC, a major concern would be connectivity
  between the computers and operating departments located
  at alternate or backup facilities.  DFAS-KC will use
  dial-up connections between locations to provide this
  connectivity.

- Voice--Voice communications are in place at the DFAS alternate processing site. Adequate voice communications facilities is a criteria for selecting the alternate facilities for the operating departments. The alternate communications numbers will be determined at time of disaster. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 172)

Telecommunications equipment, to be installed and maintained at the DFAS-KC alternate site, is listed within the plan.

### 14. Supplies

Vendors and the supplies they provide are identified within the contingency plan. A sampling of necessary supplies includes:

- PC tables

- File Cabinets

- Chairs

- Travel Vouchers and Claims for Reimbursement

- Pay and Leave documents

- Users and procedural manuals

- Floppy diskettes and calculator tape (DFAS-KC Draft Level III Contingency Plan, 1993, p. 70)

### 15. Transportation

The Facility Recovery Team Manager, assisted by the Support Operation Division and the Transportation Team, is responsible for the coordination and movement of personnel, equipment, and materials to DFAS-KC and DITSO-KC alternate processing sites.

Available methods of transportation include a combination of government and commercial automobiles, trucks and buses. Government air transportation, if available, is to be used for movement of personnel and supplies to distant alternate processing sites.

Personnel required to travel during the recovery operation will complete Travel Accommodations Request Forms for payment of travel and lodging expenses.

**16. Power and Equipment**

In an emergency, a doubly-redundant Uninterruptable Power Supply (UPS) will provide electrical power to the DFAS/DITSO-KC Center. Should the primary commercial electricity source be disrupted, generators located at the facility will activate, providing a near-instantaneous resumption of power.

Should the generators malfunction, a supply of lead-cell batteries, sensing a second disruption, assume the electrical requirements (load). For a limited period of time, this second, on-site backup system would provide sufficient electrical power for users to save/backup work currently in progress, minimizing data losses.

## 17. Documentation

In order to efficiently conduct operations from alternate processing sites, a number of documents are made available to DFAS/DITSO-KC personnel.

These documents, and multiple copies of the disaster recovery plan, are to be maintained at the DFAS/DITSO-KC Center for use in pre-disaster training and orientation sessions. Additional documents and copies of the disaster recovery plan will be held at the off-site storage facility, to be recovered for use as reference materials during the recovery phase.

Some of the required documents and their uses are listed below:

● Users Manuals--Copies of hardware and software user documentation are stored on and off-site. These reference/instructional documents will accompany DFAS/DITSO-KC personnel to alternate processing sites.

● Wiring Diagrams--Local area network wiring diagrams, maintained by Responsible Officers and network maintenance personnel within DFAS/DITSO-KC, will be used to reconstruct damaged or destroyed LANs at the Center.

● Damage Assessment Reports--This document describes the disaster's effect on data, hardware, software and the facility. The report also contains a section in which damage assessment personnel log their estimates on the length of time before production can be resumed. Management will use recovery time estimates in reports to higher authority.

● Unit Cost and Pay Manuals--These manuals contain procedures for payment of active-duty, reserve and retired Marines as well as payments to civilian employees. The manuals also cover regulations for payment of vendors should services/supplies be required in an emergency situation.

- Personnel Rosters--Used for notification of DFAS/DITSO-KC personnel during the disaster. These rosters are made up of names, addresses and telephone numbers of DFAS/DITSO-KC management, personnel and recovery teams. Also listed are mailing addresses, facsimile numbers and electronic mail addresses of vendors, alternate processing sites and Points of Contact. (DFAS Draft Level III Contingency Plan, 1993, p. 70)

**18. Plan Maintenance**

Detailed maintenance procedures within the DFAS/DITSO-KC disaster recovery plan call for periodic reviews and revisions to reflect changes in plans and policies, as well as recovery team personnel turnover. Changes are to be submitted in writing to the Recovery Coordinator for review.

The DFAS/DITSO-KC philosophy on disaster recovery plan maintenance is as follows:

...a disaster recovery plan is only as valid as the information it contains. To ensure that the plan is used effectively in an emergency it must be accurate, timely, and complete. It is imperative, therefore, that the plan be reviewed often and updated as necessary. (DFAS Draft Level III Contingency Plan, 1993, p. 70)

The plan is scheduled for annual review during January with periodic section reviews to be conducted throughout the calendar year.

## 19. Plan Testing

Disaster recovery plans, though constructed with painstaking detail over hundreds of man-hours, are virtually useless if not tested. Toigo states:

> Disaster recovery plans should not be tested in use. That is, a disaster should not have to occur before erroneous conclusions and errant strategies are revealed. (Toigo, 1989, p. 217)

If a disaster occurs before the plan is tested under practice conditions, the plan may fail miserably in execution becoming a disaster in and of itself.

Disaster planning experts, including those who owe their expertise to having recovered from "smoke and rubble-type" disasters, argue that testing is the most important element of disaster recovery planning.

Organizations that had not tested their contingency plans prior to a disaster encountered problems. For example, a Canadian fim, after experiencing a fire that demolished company headquarters, packaged over 10,000 reels of tape containing payroll systems and data and formed a caravan headed for a "hot site" located in New Jersey.

At the border they were prevented from entering the U. S. by customs agents, who were concerned that the software and checks could be used for illegal purposes. It took the intervention of the company CEO, in conjunction with the U. S. consulate, to straighten out the matter. (Toigo, 1989, p. 202)

### a. DFAS/DITSO-KC Plan Testing

DFAS/DITSO-KC has prepared four practice tests which scrutinize different portions of the disaster recovery plan. Tests are divided into three levels, arranged in order of personnel/resources required to execute the test.

Each test will be closely monitored by a team of DFAS/DITSO-KC evaluators. Extensive debriefs of test participants, stressing lessons learned during the testing evolution, are scheduled to follow each exercise. Test levels, objectives and procedures are listed in the following paragraphs:

Test 1, Level 2 Objectives--Test 1 determines:

- The adequacy of off-site storage, file availability and documentation needed for recovery.

- The completeness of Disaster Alert, Assessment, Verification and Personnel Notification procedures.

- The aggregate number of Recovery Team personnel who are available under no-notice, practice conditions, and the accuracy of telephone rosters.

Procedures--After notification of a practice disaster scenario restricting access to office files and documentation, Recovery Management Team members move to the CCC. Once there, they execute disaster assessment and evaluation procedures and determine the level of disaster plan activation. Recovery Team members, contacted at home, refer to their personal copies of the disaster plan and comply with individual/team recovery procedures.

Test 2, Level 1 Objectives--This test examines:

- Systems restoration using in-house systems, personnel and off-site files/documentation.

- The availability/applicability of critical resources to be used at alternate processing sites.

Procedures--Alerted in advance, a minimum number of Recovery Team members, responsible for critical function restoration, travel to the alternate processing site. While at the alternate site, critical functions are restored and resources checked against the Critical Resources Report to ensure adequate supplies are available to perform the test function.

Test 3, Level 1 Objectives--Conducted annually, this test evaluates DITSO-KC off-site backup procedures.

Procedures--Accompanied by an evaluator from the Recovery Management Team, DITSO-KC recovery team members travel to the off-site storage facility to check the material condition and availability of systems restoration backup tapes.

Test 4, Level 3 Objectives--The Test 4 scenario denies access to DFAS/DITSO-KC Center. Conducted annually, the test checks:

- Operation of the telecommunication network between DFAS-KC and DITSO-KC alternate processing sites.

- Restoration of critical functions, using only backup data.

Procedures--Test 4 requires the participation of DFAS-KC's Finance and End User Interface Teams and DITSO-KC Recovery Team members. The Finance Team travels to the DFAS-KC alternate processing site, while the End User Interface Team and DITSO-KC Recovery Team personnel relocate to DITSO-KC's "hot" site, Camp Lejeune, North Carolina.

DFAS/DITSO-KC evaluators will be present at both locations. During the week-long test, all critical functions, listed in the Critical Functions Report, are to be recovered via telephonic means between the alternate processing sites. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 936-954)

## D.  IMPLEMENTATION PHASE

The implementation phase describes procedures to be followed when it has been determined to activate the disaster recovery plan, and moves the organization from the non-emergency preparation phase into actual activation of the disaster recovery plan.

Depending on the amount of advance notice and type of disaster, transition to this phase may be a smooth and natural process. However, unforeseen or unforecasted disasters may find organizations implementing this phase of their disaster recovery plans with little or no lead time. (Hural, 1992, p. 11)

The implementation phase, or the evacuation phase
(Toigo), is the litmus test for recovery teams formed during
the preparation phase.

There are three functional requirements to this phase:

1. The emergency must be met with an adequate response,
ranging from use of an extinguisher to suppress a small
fire, or in a phased disaster scenario, to evacuating
hardware hours before a hurricane strikes. In a phased
disaster situation warnings may be issued well in advance
of an actual disaster.

2. Assess damage caused by the disaster and determine
whether disaster declaration criteria have been met. If
the coordinator has determined the maximum amount of time
that the organization can be without critical or vital
operations (48 hours in the case of DFAS/DITSO-KC), then
this might be the criterion for declaring a disaster. To
make this determination, site damage will need to be
accurately assessed and realistic recovery time frames
estimated.

3. Declare a disaster and invoke the plan. (Toigo,
1989, p. 162)

### 1. Plan Organization

For ease of use during this phase, the DFAS/DITSO-KC

disaster recovery plan is divided into three primary

sections: the Administrative Plan, Action Plan, and

Reference Information Section. These sections are described

below:

- Administrative Plan--Contains the non-procedural
  portions of the disaster recovery plan. It is intended
  to be used as an educational and training tool. The
  Administrative Plan also contains the Business
  Resumption Program Overview, Business Resumption Program
  Documentation, Plan Activation procedures and an
  Appendix.

- Action Plan--This team-oriented section details the specific responsibilities and procedures that recovery personnel would follow in the event of a disaster. The Action Plan segment contains team-specific information such as: team charter, team composition, notification, react and support procedures and team attachments. Each action plan component is composed of a text file, data base report and/or graphics file.

- Reference Information Section--This section contains reference information. While not vital to the recovery effort, it may be useful during the development and ongoing maintenance of the plan. (DFAS Draft Level III Contingency Plan, 1993, p. 187)

## 2. Using the Plan

An abbreviated, instructional section is contained within the plan, describing initial actions all DFAS/DITSO-KC personnel are to take at the time of a disaster. These actions are:

- Follow the DFAS/DITSO-KC Center emergency response procedures to ensure the safety of the employees, visitors, and guests, and to protect the assets of the DFAS/DITSO-KC Center.

- Designated First Alert Notification Contacts will follow Plan Activation procedures located in the Administrative section of the disaster recovery plan.

- Recovery Team members will comply with their specific recovery procedures in the appropriate Action Plan section. (DFAS Draft Level III Contingency Plan, 1993, p. 188)

## 3. Disaster Alert Overview

The graphic activation flow represented in Figure 3 depicts the DFAS/DITSO-KC First Alert Response and steps required prior to activation of the DFAS/DITSO-KC disaster recovery plan. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 198)
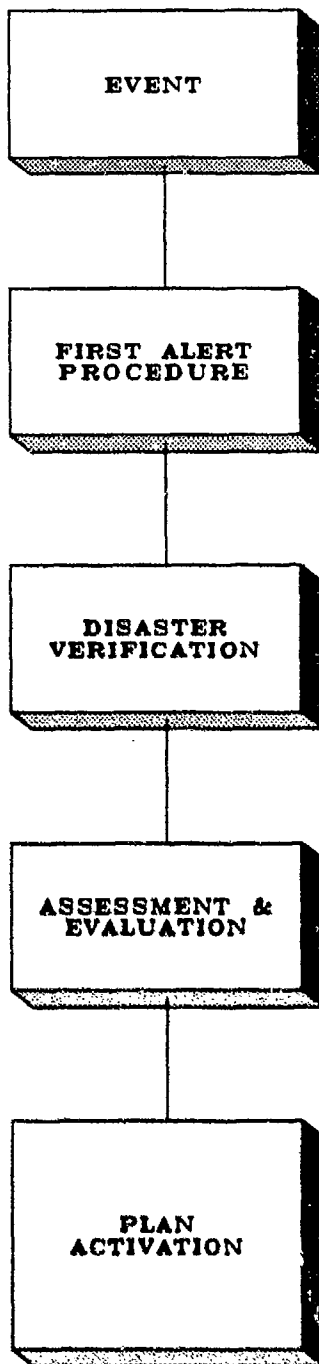
Figure 3. Disaster Alert Overview

## 4. First Alert Response

Once a disaster, or any physical event (as described in the Disaster Alert Overview) occurs, the First Alert procedures described below ensure that management, recovery teams and security personnel are appropriately notified following any potentially disastrous event. These procedures are also to be used if a non-emergency problem is to be upgraded into a disaster alert.

Anyone (a DFAS/DITSO employee, bystander, etc.) may perform initial First Alert functions by contacting DFAS/DITSO-KC Security personnel on duty at the Center. First Alert procedures are:

1. Complete steps required by existing emergency response procedures.

2. Determine if the disaster has affected the DFAS/DITSO-KC Center area.

3. If the Center area has been affected, notify one of the individuals designated as an Initial Response Contact, and provide your name, a description of the disaster, any knowledge you may have of damages and injuries, and the telephone number and location where you can be reached. (DFAS Draft Level III Contingency Plan, 1993, p. 200)

First Alert procedures are followed by a three-tiered problem review and escalation procedure, as follows:

1. Disaster verification.

2. Damage assessment and evaluation.

3. Plan activation. (DFAS-KC Draft Level III Contingency Plan, p. 200)

102

## 5. Disaster Verification

This procedure mobilizes personnel identified as Initial Response Contacts within the plan. Initial Response Contacts are DFAS/DITSO-KC management personnel at the division manager level or higher.

### a. *Initial Contact Procedures*

The first person notified of the disaster assumes responsibilities as the Initial Response Contact, and obtains and records information such as: caller identification, nature and severity of the event and the caller's preliminary estimate of damage and injury. The Initial Response Contact relieves the caller from further responsibilities and begins a preliminary assessment of the event.

When the Initial Response Contact has determined that a disaster situation exists, the Recovery Management Team will be notified and directed to report to the Crisis Coordination Center (CCC). Should the Center's on-site CCC be rendered unusable by the disaster, Management Team members will be advised to proceed to the alternate CCC location. (DFAS Draft Level III Contingency Plan, 1993, p. 202)

## 6. Disaster Assessment and Evaluation

During Disaster Assessment and Evaluation, the
Recovery Management Team is activated to decide whether or
not a disaster should be declared and the entire recovery
organization mobilized.  When the Recovery Management Team
members assemble at the CCC, they will perform the following
duties:

- Dispatch selected team members to reassess the extent of
  damage to the facility and its contents.

- Obtain facility and content damage reports from on-site
  management and/or local authorities.

- Obtain injury reports from on-site representatives
  and/or local authorities.

- Review findings of the reassessment activities.

- Determine whether to activate the disaster recovery plan
  or to terminate recovery activities.

- Determine the degree, or level, of disaster recovery
  plan activation appropriate to the amount of damage
  received, and the estimated amount of time that Center
  operations will be interrupted.  (DFAS Draft Level III
  Contingency Plan, 1993, p. 209)

## 7. Plan Activation

After initial damage assessments are complete, the
Recovery Manager can activate the plan at one of the three
levels listed below:

1. Temporary interruption/no plan activation--
Facilities, equipment and data are not seriously
affected; the problem can be handled by DFAS/DITSO-KC
personnel, building engineers or vendor personnel with a
minimum of processing and services outage.

2. Limited activation--Certain recovery teams, but not all, will be activated based on the affected areas and services.

3. Full activation--All recovery teams are to be activated. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 209)

The Recovery Management Team will also inform all recovery personnel that Management will provide the news media with a statement as soon as possible regarding the situation. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 210-211)

## 8. Recovery Team Responsibilities

During the implementation phase, the recovery teams selected and trained by DFAS/DITSO-KC greatly effect their organization's ability to react in an efficient and timely manner to an impending disaster.

DFAS/DITSO-KC recovery teams will comply with the Action Plan which describes specific responsibilities and procedures that recovery personnel are to follow in the event of a disaster. Specific procedures and a description of one of the recovery teams, the End User Interface Team, are listed below:

### a. Team Composition

The fourteen-member End User Interface Team is composed of DFAS/DITSO-KC employee specialists. Member skills include: Financial Systems Specialists, Financial Systems Analysts and Information Systems Specialists.

### b. *Notification/Assessment Procedures*

Upon receipt of the disaster alert, the End User Interface Team leader confirms that proper disaster verification procedures have been followed. The End User Interface Team leader, along with a copy of the End User Interface Team procedures and employee identification, immediately reports to the Crisis Coordination Center (CCC). Upon receipt of the disaster alert, the Team leader will be directed to proceed to either the primary or alternate CCC.

On arrival, the End User Interface Team leader will contact team personnel already on-site, and assist other team leaders in assessing damage to computer operations and communications. Once the preliminary damage assessment is complete, the End User Interface leader will meet with other team leaders, compare assessment notes and provide input to the Recovery Management Team on whether to activate the disaster recovery plan.

Should the plan be activated, the leader will contact remaining team members, using the telephone list enclosed in the team's portion of the disaster recovery plan. When all members have arrived, the leader will hold a team meeting and review team-specific recovery objectives and strategies prior to releasing members to their assigned recovery tasks.

Should End User Interface Team members be required to travel to alternate processing sites, travel arrangements will be provided by the Transportation Team. Tickets, itineraries, advance monies and administrative support will also be provided by Transportation Team personnel. (DFAS Draft Level III Contingency Plan, 1993, p. 301)

### c. Team Responsibilities

In the event of a disaster at DFAS/DITSO-KC Center, the End User Interface Team will:

- Provide user interface support to DITSO-KC.

- Provide system support for Accounting, Bond/Allotment, Military Pay, and Active Duty/Retired systems.

- Generate customer, employee, and end user situation statements. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 304)

### d. System Support

As noted above, a major portion of the End User Interface Team's responsibilities involve system support for operational sections within DFAS/DITSO-KC.

Examples of system support: backing up tapes/datasets of forecasted pay and check images used to generate payrolls until normal processing resumes, or ensuring that Joint Uniform Military Pay System (JUMPS) mid-month and monthly Update and Extract (U&E) data transactions are processed in a timely manner. (DFAS-KC Draft Level III Contingency Plan, 1993, p. 304)

107

## e. Team Leader Responsibilities

The End User Interface Team Leader will:

- Activate the End User Interface Team.

- Approve situation statements/reports.

- Evaluate user needs and problems requiring DITSO support.

- Coordinate all user needs with DITSO.

- Provide pay system support/interface with DITSO    (DFAS Draft Level III Contingency Plan, 1993, p. 301).

## f. Team Leader Administrative Procedures

The End User Interface Team leader, as with all recovery team leaders, is responsible for their team members' health and welfare.

The End User Team leader's administrative requirements include, but are not limited to:

- Monitoring personnel for signs of fatigue, and ensuring personnel receive sufficient rest during the recovery operation. In order for personnel to maintain maximum efficiency during the recovery period, the plan calls for a minimum of eight hours rest daily.

- The return of personnel to their homes at least every two weeks if personnel were moved to an alternate processing site.

- Monitoring costs accrued at the alternate processing site, and approval of payments for expenses incurred. (DFAS Draft Level III Contingency Plan, 1993, p. 301)

## E. RECOVERY PHASE

The last of the four plan development phases, the recovery phase, outlines procedures initiated after the disaster has occurred to bring the organization back to its original operating level.

The recovery phase restores the stricken organization to normal pre-disaster operation, and begins when the danger to personnel and the disaster's effects have been neutralized.

The amount of damage suffered by the organization determines the level of recovery required. If damage was minimal, recovery could be as easy as reestablishing electrical power and resuming work; more extensive damage may require shifting operations to an alternate processing site. (Hural, 1992, p. 12-13)

### 1. Relocation/Reentry

Toigo's equivalent phase, relocation or reentry, is similar to recovery concepts noted above. Relocation or reentry refers to two options that may confront a business following a disaster.

These options are:

1. If the original facility is salvageable, it may be possible to reenter it once cleanup and refit activities are completed.

2. If the facilities are unhabitable, or prohibitively expensive to reconstruct, the business may choose to relocate to new quarters. (Toigo, 1989, p. 168)

109

In either case, there is usually an interest in salvage, especially when expensive hardware, critical documents on-site and other company assets are involved.

Toigo specifies the following actions to be taken during the relocation/reentry phase:

- Systems Recovery--Procedures to restore critical and vital systems at emergency service levels within a specified time frame in accordance with the disaster recovery plan.

- Network Recovery--The reinstatement of voice and data communications at emergency service levels within a specified time frame in accordance with the disaster recovery plan.

- User Recovery--Procedures for recovering critical and vital user functions.

- Salvage Operations--Salvaging facilities, records and hardware.

- Relocation--Relocating emergency operations (system, network and user) to the original or a new facility, and the restoration of normal service levels. (Toigo, 1989, p. 161-162)

Toigo describes more detailed, team-oriented functions to be completed as the organization strives to return to normal, pre-disaster operations.

A partial list includes:

- Retrieving critical and vital data from off-site storage.

- Installing and testing systems software and applications at the systems recovery site.

- Identifying, purchasing and installing hardware at the system recovery site.

- Operating from the system recovery site.

- Rerouting network communications traffic to the recovery site (Toigo, 1989, p. 164-165).

## 2. DFAS/DITSO-KC Plan Usage During Recovery Phase

The DFAS/DITSO-KC Center disaster recovery plan is designed to provide, in one volume, organizational and procedural definitions required to guide the Center through a recovery period following a disaster.

The plan is organized to facilitate ease of use. The suggestions listed below are offered to assist the DFAS/DITSO-KC personnel in attaining familiarity in as short a time as possible:

- Read the section Administrative Plan--Executive Overview for a general description of the recovery process.

- Read the section Administrative Plan for a summary description of all team recovery strategies.

- Refer to the Administrative Plan--Recovery Organization to view the overall recovery organization and identify specific participants who will play key roles during the recovery process. (DFAS Draft Level III Contingency Plan, 1993, p. 195)

The DFAS/DITSO-KC plan is structured so that individual members of any recovery team can detach their specific recovery procedures from the body of the plan for quick reference, if needed.

### 3. Critical and Support Functions

Restoration of prioritized critical functions to pre-disaster operating levels is a primary task of DFAS/DITSO-KC recovery teams. In addition, recovery teams may be called upon to assist and support other departments' recovery efforts. Intra-department support functions are defined as follows:

> Tasks or support activities performed in support of other departments' recovery efforts. These recovery functions may be different than the normal scope of responsibility of this department or area. (DFAS Draft Level III Contingency Plan, 1993, p. 195)

### 4. Recovery Management Team

The Recovery Management Team, composed of directors of all the major divisions within DFAS/DITSO-KC Center, plays a key role in the recovery effort. Figure 4 shows the organizational structure of the Recovery Management Team. (DFAS Draft Level III Contingency Plan, 1993, p. 175)
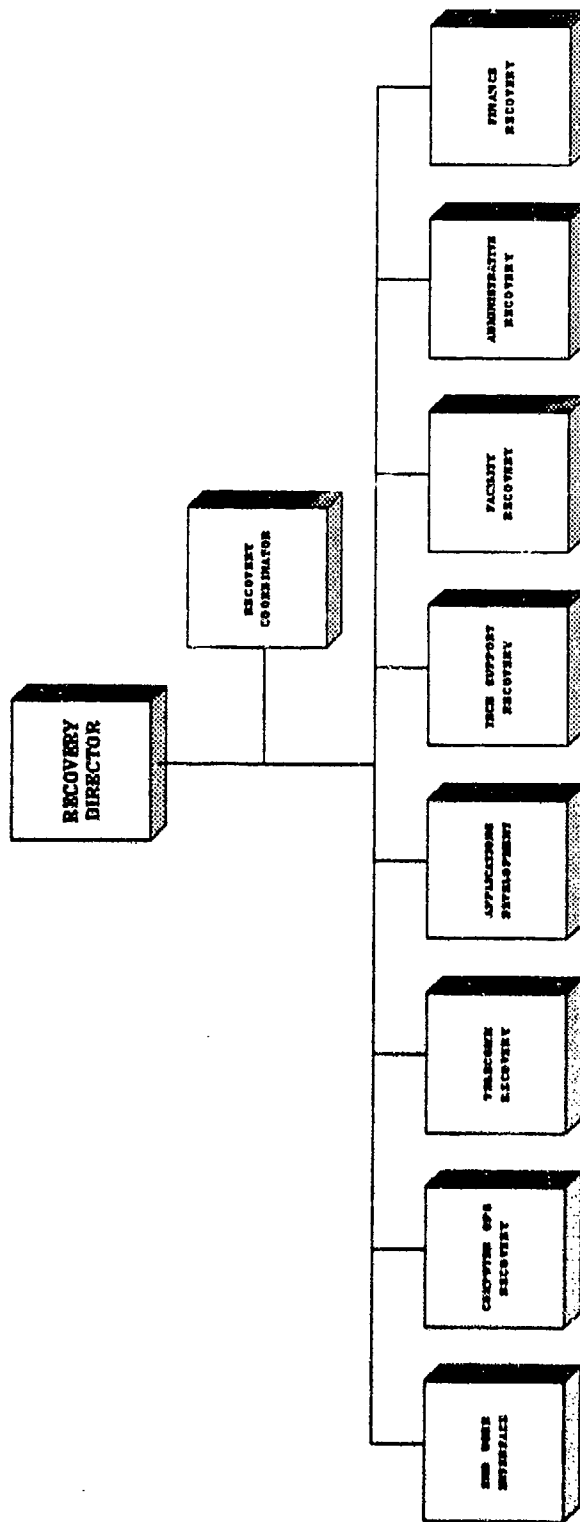
Figure 4. Recovery Management Team

113

### a. *Team Duties and Responsibilities*

Selected Recovery Management Team members' duties during the re overy phase are listed below:

- Recovery Director--Direct all recovery operations. Notify executive management of the disaster situation and recovery plan activation activities, conduct recovery operation activation meetings and establish recovery operation objectives.

- DITSO-KC Computer Operations Manager--Activate the required Computer Operations recovery teams, initiate the recovery processing site disaster alert notification, direct processing recovery activities, and direct all data retrieval, reload and recovery activities.

- Director, Information Management--Activate the required application recovery teams, support Operations with the recovery of systems data and the restart of applications and direct any programming changes required for production software or programs. (DFAS Draft Level III Contingency Plan, p. 182-183)

### 5. Alternate Site Processing

If the Recovery Management Team determines that damage has rendered the facility unusable, personnel and equipment will then migrate to alternate processing sites, establish communications, and begin the recovery process. DFAS/DITSO-KC alternate processing site strategies are listed below:

### a. *DFAS "Cold Site" Operations*

The primary DFAS-KC "cold site" is an unused warehouse in the greater Kansas City metropolitan area. This site is scheduled to house several critical DFAS-KC functions. Due to space limitations, several other cold

114

sites are to be acquired for DFAS-KC operations that are unable to use the primary cold site. These additional cold sites will be used for an estimated two to three weeks.

Additional supplies and equipment for use at the primary and alternate cold sites will be acquired and distributed by a team established for that purpose. (DFAS Draft Level III Contingency Plan, 1993, p. 172)

### b. DITSO "Hot Site" Operations

Should a disaster render the DITSO-KC Center unusable, DITSO-KC will shift operations to its designated "hot site", the Marine Corps Data Processing Facility at Camp Lejeune, North Carolina. Connectivity between DFAS-KC and DITSO-KC will be provided by dial-up telephone connections, using the Defense Switched Network (DSN). Modems, FAX machines, and other telecommunications equipment will be installed at DFAS-KC alternate sites to establish communications between DFAS-KC and DITSO-KC alternate processing sites.

DITSO-KC's hot site serves as an alternate processing site for a number of other Marine Corps Data Processing facilities. If forced to relocate to Camp Lejeune, DITSO-KC personnel would operate under guidelines set by the Transportable Contingency Action Plan (TCAP), a document containing procedures to follow should relocation be necessary due to a disaster.

Camp Lejeune offers the following hot site services:

- Logical Host Services.

- DASD (Direct Access System Device).

- Consoles.

- Work Stations.

- Printers and other peripheral devices.

- Tape Drives.

- Points of Contact to assist in the resumption of operations.

Camp Lejeune possesses sufficient computing resources to "split" its operations and provide data processing support to affected organizations. Incoming personnel will have billeting and messing services provided by tenant activities. (Interview, MSgt Spaulding, USMC, 1993)

### c. Alternate Site Lessons Learned

Camp Lejeune Data Center supervisory personnel stated that facilities that had conducted successful alternate site contingency planning exercises at the Lejeune facility all seemed to have the following common characteristics:

- Updated TCAPs that meet Marine Corps standards and guidelines.

- Visiting facilities sent their most experienced data processing personnel to participate in the exercises.

- Data Set names were correct and conformed to established standards.

- During the exercises, visiting facilities transported all of their backup data files to the "hot site", testing the completeness and accuracy of their data backup routines.

- Facilities had tested their TCAPs, on a stand-alone basis, prior to relocating to Camp Lejeune. (Interview, MSgt Spaulding, USMC, 1993)

## F.  CONCLUSIONS

### 1.  Advantages

The DFAS/DITSO-KC disaster recovery plan is a well-prepared, single-source document containing all of the pertinent reference sources and procedures for recovery personnel to use in the event of a disaster at the Center. As such, it has many advantages for the user.  They are:

a.  A concise set of instructions, separated by Recovery Team, are easily located within the plan.  Instructions are not covered in excessive detail, and do not mask the plan's true intent.  As written, these instructions should enable the plan user to function efficiently at the time of a disaster.

b.  The plan is easy to read and understand.  Commonly-used terms, vice complex acronyms and abbreviations, are used throughout the document.

c.  Initial contact telephone numbers are listed with each individual recovery team.  Each recovery team member is listed with primary and alternate numbers to be used by contact personnel.

d.  Logistical requirements for personnel deploying to alternate processing sites are well-defined within the plan.

e.  Critical functions, in order of priority, have been identified by DFAS/DITSO-KC.  Following a disaster, these functions are to be restored in order of importance, restoring the Center to pre-disaster operating levels.

## 2. Disadvantages

No plan is without disadvantages. While the DFAS/DITSO-KC plan is an extremely well-prepared document, showing insight and care in its preparation, there are areas that could be improved, as listed below:

a.   Telephone numbers and individual names are listed within the body of the document.  Should names/numbers change, it will be a complex administrative burden to alter the plan to reflect them.  Placing information of this sort in an Appendix would make the change process much easier.

b.   The DFAS/DITSO-KC disaster recovery plan is massive, consisting of nearly 1000 pages of printed material.  To the first-time user, the plan would appear intimidating due to its sheer bulk.  Efforts are being made to condense/remove redundancies.  In future, team members will only retain for reference those portions of the plan that pertain to their specific recovery team.  Complete copies of the plan will be retained at each workcenter and in off-site storage.

c.   There is inadequate guidance pertaining to the transfer of backup data from off-site storage to alternate processing sites.  This is an area that should be rehearsed in a benign, non-disaster setting.  Backup data is especially vulnerable during transport if adequate protection is not provided.

## VII. SUMMARY

### A. THESIS PURPOSE

This thesis has analyzed disaster recovery planning at three DOD computer facilities: the DFAS/DITSO Kansas City Center and two U. S. Air Force organizations.

Of particular interest was the impact of contingency planning measures at Clark AFB, Philippines and Homestead AFB, Florida following significant natural disasters. Worthwhile characteristics of these disaster plans were discussed at length; equally as important was the examination of how these plans could have been more effective.

From this evaluation, lessons learned have been documented that should help DOD information managers to identify and correct possible weaknesses in their facilities' disaster recovery plans.

### B. LESSONS LEARNED

#### 1. DFAS/DITSO-Kansas City

Each selected facility had prepared a disaster preparedness plan. Of these, DFAS/DITSO-KC was engaged in a complete reconstruction of their existing planning document. This reconstruction resulted in a comprehensive contingency plan that appears to meet their requirements.

The new DFAS/DITSO-KC plan has many advantages. It is easy to read and understand. Instructions and procedures are not covered in excessive detail and do not mask the plan's true intent.

Toigo (1989) stated that a disaster plan is only as good as the testing that accompanies it. DFAS/DITSO-KC planners have prepared a detailed series of tests to check the plan's effectiveness during a number of practice disaster scenarios. These tests will evaluate alternate site operations, backup data recovery and other criteria. Supervisory personnel are to monitor, evaluate and debrief each test.

The DFAS/DITSO-KC plan contains minor procedural and administrative disadvantages. Planners are in the process of rectifying administrative drawbacks; realistic testing should resolve procedural deficiencies.

## 2. Clark Air Force Base

Clark Air Force Base contingency planning was severely tested by the eruption of Mount Pinatubo.

Until the spring of 1991, the Clark Data Processing Center had not considered volcanoes as a threat to the facility. It was a reasonable assumption, in that nearby Mount Pinatubo had not shown any signs of activity for over 200 years.

Lacking formal guidance, the innovative "Volcano Plan" was formulated by an experienced DPC computer technician to cope with Mt. Pinatubo's eruption.

Problems were encountered in obtaining satellite communications during the recovery effort. The Volcano Plan worked well but was hampered by the cancellation of alternate site operations.

Disregarding the obstacles encountered, the DPC's recovery from "the eruption of the century" was a success. Miraculously, no lives were lost. The facility resumed processing operations and backup data were preserved.

This success was largely due to the bravery and professionalism of the mission-essential team that remained behind at Clark. Adapting to danger, adversity and the base's uncertain future they safeguarded vital backup data, activated alternate site operations and resumed processing in a timely manner.

Unfortunately, their efforts were for naught. Clark's future had been in doubt for years by the time the volcano blew. Coming in the middle of U. S.--Philippine basing rights negotiations, the explosion only hastened what may have been inevitable--the abandonment of Clark AFB.

### 3. Homestead Air Force Base

The devastation of the Homestead Base Communications and Computer Center (BCCC) and the subsequent recovery operation should provide much useful information for DOD contingency planners.

The BCCC was well prepared; hurricanes were identified as a threat to the facility and appropriate measures were in place to safeguard the facility's personnel and equipment.

The BCCC's Emergency Action Procedures (EAP) were regularly tested. The plan was updated to reflect the Regionalization of the BCCC and was current at the time of the hurricane. The facility appeared able to withstand a disaster.

Notified of the approaching hurricane, well-trained BCCC personnel installed specially-made plastic covers over computers and communications equipment, secured classified materials and evacuated the facility prior to the storm.

However, no amount of disaster planning and preparation could have protected the BCCC from Hurricane Andrew, the most destructive natural disaster in U. S. history. (Gore, 1993, p. 15)

The storm devastated Homestead's data processing facility, ripping off most of the roof and soaking the interior with rainwater. Environmental control equipment (air-conditioners and humidifiers) was damaged; exposed to the elements, plastic-covered equipment retained moisture and corroded in the humid Florida environment.

Even though the Homestead facility was severely damaged, BCCC disaster planning measures were effective. Backup data were saved, processing promptly resumed and, most importantly, no lives were lost.

BCCC personnel proved that disaster preparedness training pays off. The airmen that secured the facility knew their responsibilities, followed EAP procedures and carried out their duties without hesitation.

Regional commands demonstrated high levels of cooperation. Homestead functional users relocated to MacDill and Patrick AFBs and resumed operations not yet performed by the Regional Processing Center.

Bureaucratic snarls were avoided; communications links were routed to MacDill and Patrick, facilitating data transmissions with the Gunter RPC.

Above all, Hurricane Andrew proved the utility of the Regionalization concept. Prior to the storm, most of Homestead's computer assets had been relocated to the Gunter RPC. Therefore, most of the customary disaster recovery steps--and the associated delays--were avoided.

Via an established communications link, data were backed up and stored on a regular basis. Homestead's functional users were able to migrate to the Gunter RPC, access their backup data and quickly resume operations.

The aftermath of the storm revealed a weakness in the regional processing concept, the lack of an alternate processing site for the Gunter RPC. Had Gunter, the first of five planned RPCs been disabled it would have crippled Air Force data processing operations in the Southeastern United States. RPCs will ultimately act as each other's backup sites, but until more are completed, difficulties would arise should an RPC be destroyed.

# APPENDIX

## DISASTER RECOVERY PLAN OUTLINE

A. PLANNING PHASE
   1. Preliminary Planning
   2. Plan Development
   3. Critical/Vital Functions


B. PREPARATION PHASE
   1. Purpose
   2. Scope
   3. Objectives
   4. Assumptions
   5. Physical Inventory
   6. Risk Assessment
      a. Data Collection and Analysis
      b. Environmental Hazards
   7. Backup Operations
   8. Off-Site Storage
   9. Alternate Site Processing
   10. Recovery Team Personnel and Training
   11. Hardware and System Software
   12. Communications
   13. Supplies
   14. Transportation
   15. Power and Equipment
   16. Documentation
   17. Plan Maintenance
   18. Plan Testing


C. IMPLEMENTATION PHASE
   1. Plan Organization
   2. Using the Plan
   3. Disaster Alert Overview
   4. First Alert Response
   5. Disaster Verification
   6. Disaster Assessment and Evaluation
   7. Plan Activation
   8. Recovery Team Responsibilities
      a. Team Composition
      b. Notification/Assessment Procedures
      c. Team Responsibilities
      d. Team Leader Responsibilities

     e.   Team Leader Administrative Procedures

D.   RECOVERY PHASE
    1.   Relocation/Reentry
    2.   Critical and Support Functions
    3.   Alternate Site Operations
       a.   "Cold Site" Operations
       b.   "Hot Site" Operations

# LIST OF REFERENCES

Anthes, G. H., "IS Blunts Hurricane's Impact,"
Computerworld, p. 6, 31 August 1992.

Anthes, G. H., "IS Helps Rebuild After Andrew,"
Computerworld, p. 6, 7 September 1992.

Barela, T., "Addressing the Future," Airman Magazine, p. 8,
November 1992.

Dacaney, B. M., Mt. Pinatubo 500 Years After, Mass Media
Publishing Corporation, 1991.

Defense Finance and Accounting Service, Draft Level III
Contingency Plan for DFAS-KC, p. 2-936, 22 February 1993.

Defense Information Systems Agency, Memorandum for Director,
Defense Finance and Accounting Service-Kansas City, 18
December 1992.

Defense Finance and Accounting Service, Minutes of
Contingency Plan Working Group, 9 December 1992.

Defense Finance and Accounting Service, Minutes of DFAS
Contingency Planning Working Group, 5 November 1992.

Defense Finance and Accounting Service, Memorandum for
Deputy Directors, Center Directors, and General Counsel, 30
November 1992.

Department of the Air Force, 1961st Communications Group,
Data Processing Center, Clark Air Force Base, Republic of
the Philippines, Operating Instruction 123-1, Disaster
Recovery Plan, 1 October 1988.

Fisher, S. E., "PC Users Glean Lessons from Trade Center
Blast," PC Week, p. 10, 8 March 1993.

Gillert, G., "DOD Spearheads Relief," Air Force Times, p.
52, 14 September 1992.

Gillert, G., "Homestead Sagas," Air Force Times, p. 12-15,
14 September 1992.

Gore, R., "Andrew Aftermath," <u>National Geographic Magazine</u>, p. 10-37, April 1993.

Grier, P., "Last Days at Clark," <u>Air Force Magazine</u>, February 1992.

Haggerty, M. J., "Andrew's Wrath...Wake of the Storm," <u>Airman Magazine</u>, p. 2-9, November 1992.

Hoffman, N. H., "Explosion Spotlights LAN Vulnerability," <u>Computerworld</u>, p. 67, 15 March 1993.

Hural, P. J., <u>Comparative Assessment of U. S. Marine Corps Disaster Recovery Plans for Information Systems</u>, Master's Thesis, Naval Postgraduate School, Monterey, California, September 1992.

Interview between J. Licci, MSgt, USAF, Standard Systems Center, Computer Operations Directorate, Maxwell Air Force Base, Gunter Annex, Alabama, and the author, 25 February 1993.

Interview between C. Reidy, SSgt, USAF, Data Processing Activity, Andersen Air Force Base, Guam, and the author, 28 February 1993.

Interview between C. Moore, Captain, USAF, Homestead Air Force Base, Florida, and the author, 10 March 1993.

Interview between R. H. Reed, CMSgt, USAF, Standard Systems Center, Computer Operations Directorate, Maxwell Air Force Base, Gunter Annex, Alabama, and the author, 28 January 1993.

Interview between J. Compton, LtCol, USAF, Standard Systems Center, Computer Operations Directorate, Maxwell Air Force Base, Gunter Annex, Alabama, and the author, 29 January 1993.

Interview between Facility Manager, DFAS/DITSO Kansas City, Missouri, and the author, 22 December 1992.

Interview between J. Spaulding, MSgt, USMC, Camp Lejeune, North Carolina, Database Administration Section, and the author, 25 February 1993.

Interview between J. Buckner, Director of Computer Operations, Gunter Air Force Base, Alabama, and the author, 26 January 1993.

Interview between Disaster Recovery Planners, DFAS/DITSO Kansas City, Missouri, and the author, 22 December 1992.

Leeke, J., "Bomb Teaches Lessons in Planning," MacWeek, April 12, 1993.

McPartlin, J. P., "Down and Out in Miami," InformationWeek, p. 12-13, 31 August 1992.

Toigo, J. W., Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems, Prentice-Hall, Inc., 1989.

U. S. Marine Corps, Camp Lejeune, North Carolina, Database Administration Section, Transportable Contingency Action Plan, 8 April 1991.

# INITIAL DISTRIBUTION LIST

|  |  | No. Copies |
|--|--|:--:|
| 1. | Defense Technical Information Center<br>Cameron Station<br>Alexandria VA 22304-6145 | 2 |
| 2. | Library, Code 052<br>Naval Postgraduate School<br>Monterey CA 93943-5002 | 2 |
| 3. | Commandant of the Marine Corps<br>Code TE 06<br>Headquarters, United States Marine Corps<br>Washington, D. C. 20380-0001 | 2 |
| 4. | Professor William Haga<br>Naval Postgraduate School, Code AS/HG<br>Monterey, CA 93943-5000 | 1 |
| 5. | DFAS Disaster Head<br>DFAS-KC<br>Code MM<br>1500 E. Bannister Road<br>Kansas City, MO 64197-0001 | 1 |
| 6. | Master Sergeant Joseph Licci<br>Standard Systems Center/SSMLB<br>Maxwell AFB, Gunter Annex<br>Montgomery, AL 36114-3218 | 1 |
| 7. | Major John D. Harrigan<br>P. O. Box 345<br>Girard, KS 66743 | 2 |
| 8. | Captain Chris Moore<br>31st Communications Squadron/CC<br>Homestead AFB Contingency Operations<br>Miami, FL 33218-0001 | 1 |
| 9. | Professor Roger Stemp<br>Naval Postgraduate School, Code CS/Sp<br>Monterey, CA 93943 | 1 |