APPENDIX D

Networx Enterprise Program

Contract Number TQC-JTB-05-0002

Networx Disaster Recovery Plan

Prepared by

AT&T
3033 Chain Bridge Road
Oakton, Virginia 22185
USA

REVISION HISTORY

DATE	VERSION	REVISION/CHANGE DESCRIPTION
10/24/05	1.0	Initial release
7/14/2006	1.1	Updated for Amendment 5 and CRs and DNs
3/5/07	1.2	Final Proposal Revision

SIGN-OFF

Author:	_____	_____
	Name	*Date*
Disaster Recovery Manager:	_____	_____
	Name	*Date*
Program Manager:	_____	_____
	Name	*Date*

TABLE OF CONTENTS

LIST OF FIGURES iii

LIST OF TABLES iv

List of Acronyms v

1.0 Overview 1

2.0 Disaster Recovery Organization 2

2.1 The Network Disaster Recovery Team 2
2.2 Disaster Recovery Liaison Officer (NS/EP Emergency Liaison Officer) 5
2.3 Other Organizational Units 6
2.3.1 The Global Network Operations Center 6
2.3.2 Special Operations Team 8
2.3.3 On-Site Work Force 10
2.3.4 Disaster Engineering Connection Technology 10

3.0 Disaster Recovery communication 12

3.1 Major Failure Notification Process 12
3.2 AT&T Internal Communication 12
3.3 Communication with the Government 14
3.4 Communication to Critical Government Locations 14
3.5 Communication with Suppliers, Partners, and Other Networx Stakeholders 15
3.5.1 Cingular 15
3.5.2 Global Crossing 16
3.5.3 Other Networx Stakeholders 17

4.0 Disaster Recovery Strategy 17

4.1 AT&T Strategy 17
4.2 Cingular Strategy 21c
4.3 Global Crossing Strategy 23
4.4 Telenor Satellite Services 24

5.0 Disaster Recovery Capabilities 24

5.1 Management Capabilities 26

5.2 Technical Capabilities 28
5.3 Operational Capabilities 36b
5.4 Cingular Capabilities 37
5.5 Global Crossing Capabilities 38
5.6 Summary of Recent AT&T Recovery Deployments 39

6.0 Disaster Recovery Readiness/Preparedness 41

6.1 Annual Preparedness Drills 42

Attachments 45

AT&T Disaster Recovery Example Deployments 45
Cingular Disaster Recovery Example Deployments 50
Global Crossing Disaster Recovery Examples 54

LIST OF FIGURES

Figure 2.1-1: The AT&T Disaster Recovery Process. 4
Figure 2.3.1-1: AT&T's GNOC Global Wall Display. 6
Figure 2.3.2-1: AT&T HazMat Team. 8
Figure 2.3.4-1: AT&T Disaster Engineering Connect Technology (DECT) High-Level Architecture. 11
Figure 4.1-1: AT&T's Survivability Protocol. 20
Figure 5.0.3-1: AT&T's Response to World Trade Center Disaster. 26
Figure 5.1-1: Network Disaster Recovery Solutions. 27
Figure 5.2-1: Backbone Network Disaster Recovery Configuration. 28
Figure 5.2-2: 4ESS Disaster Recovery Configuration. 30
Figure 5.2-3: ATM Recovery Architecture. 31
Figure 5.2-4: Frame Relay Recovery Architecture. 31
Figure 5.2-5: Local Network Services Recovery Trailer Plan. 32
Figure 5.2-6: IP Trailer and Functional Architecture. 33
Figure 5.2-7: Intelligent Optical Network Architecture. 34
Figure 5.2-8: AGN Network – EMEA. 35
Figure 5.3-1: An Emergency Communication Vehicle (ECV) at the World TradeCenter Police command center in September 2001. .....36c
Figure 6.0-1: Shifting Paradigms: Zero Application Downtime. 42
Figure A-4: An ECV deployed adjacent to the World Trade Center, September 2001. 49
Figure A-5: An NDR Emergency Communications Vehicle (left) and an NDR phone bank at a Red Cross shelter in Kirby, Texas (right). 50

LIST OF TABLES

Table 2.1-1: National Disaster Recovery Team. 3
Table 2.1-2: A six step method. 5
Table 4.1-1: The AT&T Reaction Time Sequence. 19
Table 4.1-2: AT&T Recovery Strategy for Critical Network Elements. 19
Table 4.3-1: The Global Crossing Team Ranks Disasters. 23
Table 4.3-2: Global Crossing DR process. 24
Table 5.6-1: Network Disaster Recovery Recent Deployments. 40
Table 6.1-1: DR Drills Instill Readiness. 43
Table A-1: Circuit Installation after Hurricane Katrina. 47

LIST OF ACRONYMS

ACRONYM	DEFINITION
3Ps	Predictive, Preventative and Proactive
3CPs	Communication, Command and Control
AAFES	Army Air Force Exchange Services
ACS	AT&T Consumer Services
AGN	AT&T Global Network
AT&T	American Telephone & Telegraph
ATM	Asynchronous Transfer Mode
Cm3	Communication Module Model 3
CNI	Common Network Interface
COLT	Cell on Light Truck
COR	Contracting Officer's Representative
COW	Cell on Wheels
CPO	Contractors Program Organization
CPR	Cardiopulmonary Resuscitation
DACS	Digital Access Cross-connect System
DACSR	Diversity, Avoidance & Customer Specified Routing
DCS	Digital Cross-connect Switch
DECT	Disaster Engineering Connection Technology
DHS	Department Homeland Security
DIRECT	Disaster Intelligent Recovery Engineering Connection Technology
DMS	Type of Switching
DROT	Disaster Recovery Operations Team
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DWDM	Dense Wavelength Division Multiplexing
ECV	Emergency Communications Vehicle
EDT	Eastern Daylight Time
EMEA	Europe, Middle East, and Africa
ERP	Emergency Response Plans
FACTS	Field and Center Technical Support
[redacted]	[redacted]
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
GNOC	Global Network Operations Center
HazMat	Hazardous Material
ICS	Incident Command Structure
IDLH	immediately dangerous to life or health
IMS	Incident Management System
IOS	Intelligent Optical Switch
ITSG	Infrastructure Technical Services Group
IXC	InterExchange Carrier
LEC	Local Exchange Company

LNS	Local Network Services
LONESTAR	Local Network Services Technology Automated Recovery
MCB	Management Control Bridge
MFAB	Major Failure Action Binder
MIP	Major Incident Plan
MoW	most-of-the-world
MSC	Mobile Switching Centers
MSP	Multi-Services Platform
MTSO	Mobile Telephone Switching Offices
MTTR	Mean Time To Repair
NCC	National Coordination Center
NCS	National Communication System
NDR	Network Disaster Recovery
NO	Network Operations
NOC	Network Operations Center
NS/EP	National Security/Emergency Preparedness
NYPD	New York Police Department
OSWF	On-site Work Force
PMO	Program Management Office
POP	Point of Presence
PSTN	Public Switched Telephone Network
PX	Post Exchange
RFP	Request for Proposal
RNOC	Regional Network Operations Center
RTNR	Real Time Network Routing
RTO	Recovery Time Objective
SDP	Service Delivery Point
SO	Special Operations
SONET	Synchronous Optical Network
TSP	Telecommunication Services Priority
UK	United Kingdom
WPS	Wireless Priority Service
WTC	World Trade Center

1.0 OVERVIEW

The Government receives the most reliable and survivable Networx services for their communications portfolio. AT&T's leading Disaster Recovery program is capable of handling everything from network infrastructure to applications and security. Our strategy is to restore the network and all of the associated services riding on that network or supported by that network. Any infrastructure (including human infrastructure) needed to support the services AT&T provides is accounted for in Disaster Recovery planning. AT&T has a long tradition of designing, deploying, and testing disaster recovery programs used to quickly restore all services to Government customers.

Agencies receive the best service continuity in the marketplace through an executable Disaster Recovery Plan, based on AT&T's corporate Network Disaster Recovery (NDR) Program. The NDR program and organization are responsible for business continuity planning and preparedness standards across the entire corporation. AT&T's NDR group is responsible for:

- Identifying and evaluating critical network service components
- Determining how/when redundancy is required in network configuration planning
- Regular testing of disaster recovery processes, procedures, and equipment
- Demonstrating Disaster Recovery (DR) capabilities.

NDR grew out of the need to help ensure the availability of AT&T's services, applications, and network operations centers (NOCs) through any disaster. In addressing this effort, AT&T's NDR program has become the benchmark against which the telecommunication industry is measured. NDR conducts quarterly field exercises to evaluate the effectiveness and efficiency of our disaster recovery program. The program establishes clear lines of authority

and sets standards for all required processes and tools for managing disaster deployments and drills.

A disaster can occur when a Network Office (also referred to as a Central Office) building and all associated equipment or information systems contained within are completely destroyed or rendered useless. The NDR

team is typically deployed if the restoration of service exceeds the normal capabilities of the network maintenance processes, and usually requires long-term deployment of specialized equipment and resources. The cause could be any natural or man-made event, such as:

- Hurricanes
- Floods
- Earthquakes
- Volcanic eruptions
- Fire
- Terrorism

The Government will be provided with a revised disaster recovery plan within 30 calendar days of *Notice to Proceed* and annually thereafter (on the anniversary of the contract award) for the duration of the contract. The revised plan and annual revisions are delivered to GSA in MS Word via the web, E-mail, or CD, as required.

2.0 DISASTER RECOVERY ORGANIZATION

2.1 The Network Disaster Recovery Team

AT&T's NDR Team is responsible for the rapid recovery of service at AT&T sites following a catastrophic event, such as restoring the functionality for a central office or network element within the AT&T network that has been destroyed or rendered useless. From its beginning in 1992, NDR has been chartered to develop and maintain the necessary processes for recovery of functionality at critical locations. Since then, AT&T has grown our inventory of trailer-mounted equipment to over [redacted], added pre-planned recoveries for over [redacted] and established a diverse team of

approximately [redacted] who plan and execute recovery using well-tested processes.

The NDR Team is composed of AT&T managers, engineers, and technicians specially trained in the physical recovery of AT&T's network. Team members from across the United States volunteer for this assignment, participating in several recovery exercises each year to train and to maintain their skills in using the disaster recovery equipment and processes.

A governance structure has been established to help ensure disaster recovery efforts have been given the appropriate priority, focus and resources within AT&T. **Table 2.1-1** provides a breakdown of the roles and function within the governance structure.

AT&T National Disaster Recovery Team Functions

DR Officer	• Responsible for the overall AT&T Business Continuity Program • Charged with protecting mission-critical business functions • Reports to Chairman, senior leadership team, Board of Directors
DR Council	• Senior officers of AT&T • Provide leadership and support for continuity and recovery decisions
DR Steering Committee	• Staffed with key personnel from various functional areas • Charged with managing their operations within disaster recovering standards and practices
Corporate Support Team	• Represents the common support functions across AT&T • Ensures resources are available to fully support the DR program
Incident Management Team	• Responsible for command and control • Help to ensure service continuity

Table 2.1-1: National Disaster Recovery Team. *These teams implement disaster avoidance measures and manage the prepared Disaster Recovery Plans.*

The NDR organization has developed extensive disaster recovery processes and methodologies. All NDR activities are driven by these procedures as summarized in **Figure 2.1-1.**

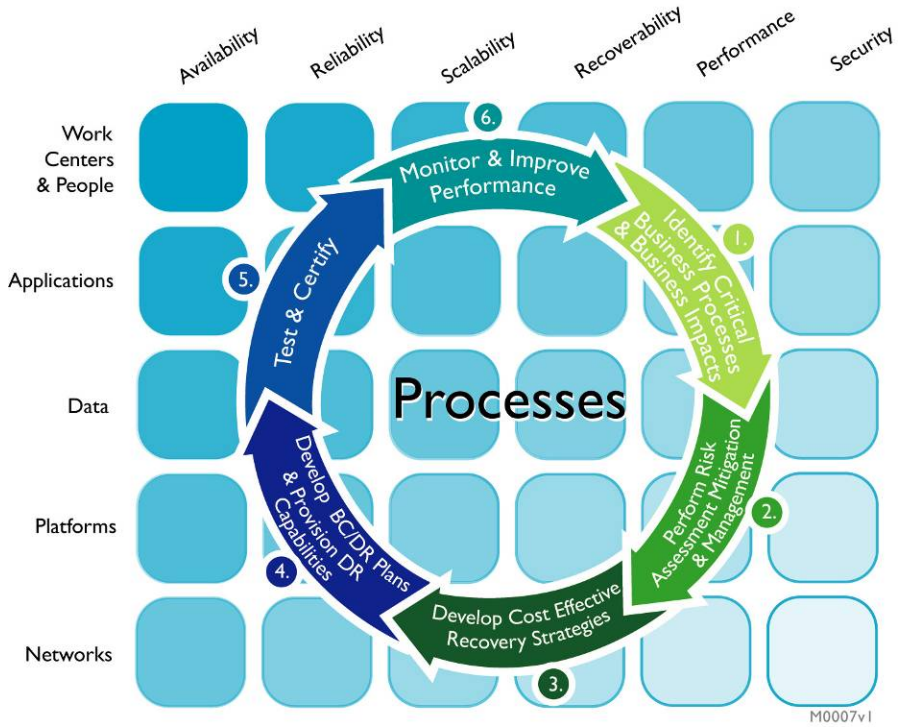


Figure 2.1-1: The AT&T Disaster Recovery Process. *A continuous cycle from assessment to testing prepares us for effective Disaster Recovery efforts.*

As shown, AT&T's process methodology employs a continuous cycle from assessment to testing. Services are continuously monitored, evaluated, and tested. These tasks are performed while taking into account all networking elements, application infrastructure, and risk/cost scenarios. With these processes as a foundation, the NDR Team utilizes a six-step Disaster Recovery Methodology as summarized in **Table 2.1-2**. This methodology forms the basis of a highly effective Disaster Recovery Plan and team able to meet Networx requirements.

SIX STEP DISASTER RECOVERY METHODOLOGY

Step	*Description*
1	Identify critical processes and impacts. This requires understanding the consequences of complete service failure scenarios and their impact on Government missions.
2	Perform risk assessment and mitigation. In this step the critical mission impacts are prioritized.
3	Develop Cost Effective Recovery Strategies. In this step AT&T identifies the recovery options, ranging from the use of existing products and processes, to newly developed ones.
4	Develop Corresponding Disaster Recovery Plans and Provision all Necessary Capabilities. This step documents the strategy that best fits the Government's requirements
5	Test and Certify. This step validates the plan by testing the equipment and processes in a live scenario.
6	Monitor and Improve Performance. This final step requires the Government and AT&T stakeholders to

keep apprised of new developments and strategies in disaster recovery planning, as well as improvement opportunities within the existing solution.

Table 2.1-2: A six step method. *Using this methodology the NDR team can map each critical business requirement to the Disaster Recovery Plan and test and document AT&T responses. As a need for improvement is identified, the six-step process begins again.*

2.2 Disaster Recovery Liaison Officer (NS/EP Emergency Liaison Officer)

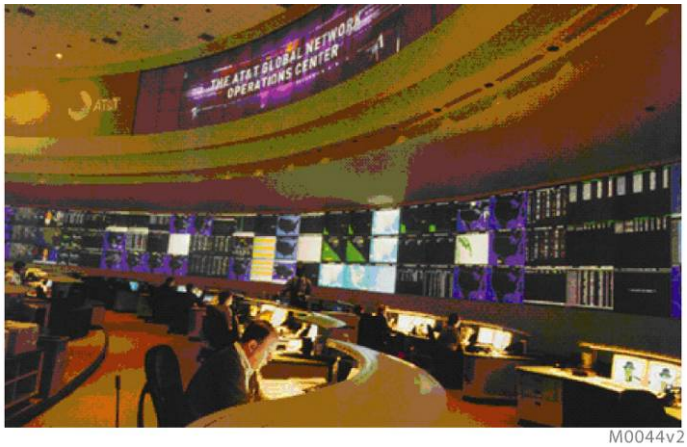
[redacted] Group Manager Network Disaster Recovery, possesses all of the required qualifications (including a current Secret clearance for discussion of classified material with Government personnel) and, as such, will perform all of the duties described in Section C.3.3.3.2.3. [redacted] has been designated as the Networx Disaster Recovery Liaison Officer. [redacted] U.S. and internationally. [redacted] AT&T NDR organization, [redacted]

[redacted] Networx Disaster Recovery Liaison Officer, [redacted] liaison officer between the Government Program Management Office (PMO) and AT&T—as well as the key link between the AT&T Networx Contractor's Program Organization (CPO) and our corporate disaster recovery resources. [redacted] PMO [redacted] RFP, AT&T [redacted] GSA's Fairfax, Virginia location [redacted] NDR team [redacted]

[redacted]NDR [redacted]PMO [redacted]PMO [redacted]PMO [redacted]PMO [redacted]PMO [redacted]PMO [redacted]AT&T [redacted]PMO [redacted]

2.3 Other Organizational Units

2.3.1 The Global Network Operations Center



M0044v2

Figure 2.3.1-1: AT&T's GNOC Global Wall Display. *AT&T uses the largest and most sophisticated command-and-control center of its kind in the world to service Networx.*

In the event of an AT&T Network Office being completely destroyed or sustaining major damage requiring lengthy repair, the Global Networking Operations Center (GNOC) activates the AT&T Network Disaster Recovery Team. Located in Bedminster, New Jersey, AT&T's GNOC is the largest and most sophisticated command-and-control center of its kind in the world (see **Figure 2.3.1-1**). On an average business day, the AT&T network carries 4.411 petabytes of data (the equivalent of transmitting the printed contents of the Library of Congress every 3.6 minutes) and approximately 300 million

voice calls. In 2004, our network's reliability performance rating ranged between 99.991 and 99.998 percent.

The GNOC staff monitors and proactively manages the data and voice traffic flowing across AT&T's domestic and global networks, 24X7. From their workstations on the GNOC floor, our staff of professionals can quickly survey a sweeping wall of 141 giant screens displaying different aspects of network activity, network topography, and news events. Each team member can monitor a different network segment or technology, using the most advanced diagnostic and management tools available.

The GNOC staff can adjust the network by temporarily increasing capacity to respond to an event or a customer need. The GNOC also uses protective controls to stop intentionally-generated and potentially harmful traffic or relieve volume-related congestion.

To ensure service reliability, the GNOC oversees the scheduling of all potential service-impacting network maintenance work or upgrades. Internal restrictions are put in place during high-traffic periods or events, preventing non-critical work from impacting performance. The GNOC provides AT&T's contingency planning for predictable network situations, including special national security events.

The GNOC also continually monitors the condition of AT&T's global network for any anomaly that threatens or impacts network performance. If such an anomaly is detected, the GNOC staff manages our response using a practiced and proven incident command process called 3CP (Command, Control, and Communications Process).

The Incident Command Team is led by the NDR Duty Officer in the GNOC, a role that is staffed 24X7. This officer coordinates the network incident

response across AT&T organizations, assessing the impact of the event in near-real time and prioritizing the restoration efforts. In response to a catastrophic event, the GNOC activates AT&T's NDR Team and coordinates its response.

2.3.2 Special Operations Team

Figure 2.3.2-1: AT&T HazMat Team. *Team members receive special HazMat training and equipment to help ensure the integrity of the network in hazardous conditions.*

The mission of AT&T's NDR Special Operations (SO) Team is to provide maintenance and/or provisioning services for the AT&T Network in immediately dangerous life or health (IDLH) environments. IDLH conditions could include chemical, biological or radiological contamination and would require use of specialized hazardous material (HazMat) response equipment and processes. The requirements and commitment needed to develop an internal HazMat response team are complex and virtually new to the industry. The SO HazMat program allows our own disaster recovery specialists to work safely in potentially hazardous environments and differentiates our disaster preparedness program from that of other networking/telecommunications companies. Refer to **Figure 2.3.2-1**.

An NDR-SO HazMat response would have one or more of the following objectives:

- Prevent a service outage through the completion of standard maintenance (repair) activities
- Prolong the duration of service to allow recovery processes to be completed
- Perform restoration activities to restore service
- Inspect and/or investigate damage to facilities.

AT&T manages SO training drills and responses using an Incident Management System (IMS) that includes specialized roles and measures unique to a HazMat response (e.g., decontamination team leader, entry, rapid intervention, air management, public health liaison). The IMS was implemented in the year 2000 and AT&T is currently one of the private-industry leaders in its use. HazMat certification requires training in the following:

- Hazard communication
- Hazardous waste operations and emergency response
- Respiratory protection
- First aid (including CPR)
- Blood-borne pathogen awareness
- Personal protective equipment
- Incident Command Structure or ICS (Officers/staff receive additional training in bio-terrorism, radiological safety, and weapons of mass destruction.

Significant time is required to achieve and maintain HazMat level certification and for maintaining competency with the specialized equipment that permits our HazMat responders to operate in actual or potential IDLH environments. This equipment includes protective clothing, self-contained breathing

apparatus, decontamination equipment, waste management equipment, and a mobile breathing air compressor.

In addition, AT&T uses environmental monitoring equipment to help ensure team members are not exposed to elevated levels of chemical, biological, or radiological agents. Finally, AT&T employs its own industrial hygienists and environmental health and safety qualified personnel as part of the SO team.

2.3.3 On-Site Work Force

In the event of a major disaster, an emergency management structure is put into place. An emergency operations center is immediately set-up and an On-Site Work Force (OSWF) is established. For example, during Hurricane Katrina, the “Katrina Situation Room” was established as a central command and control point for all hurricane related recovery efforts. As part of the emergency management structure, the OSWF is deployed to maintain and repair the various elements of the network. These personnel work in concert with various technical support and command organizations including the GNOC.

2.3.4 Disaster Engineering Connection Technology

The AT&T Disaster Engineering Connection Technology (DECT) team employs software developed by AT&T Labs specifically for the purpose of re-engineering network traffic utilizing AT&T’s trailer-mounted NDR assets. These software applications allow NDR to meet its recovery time objectives (RTO) by supplying essential Network Office data and recovery information prior to the deployment and during the operational phase of a disaster event. The DECT architecture is presented in **Figure 2.3.4-1**.

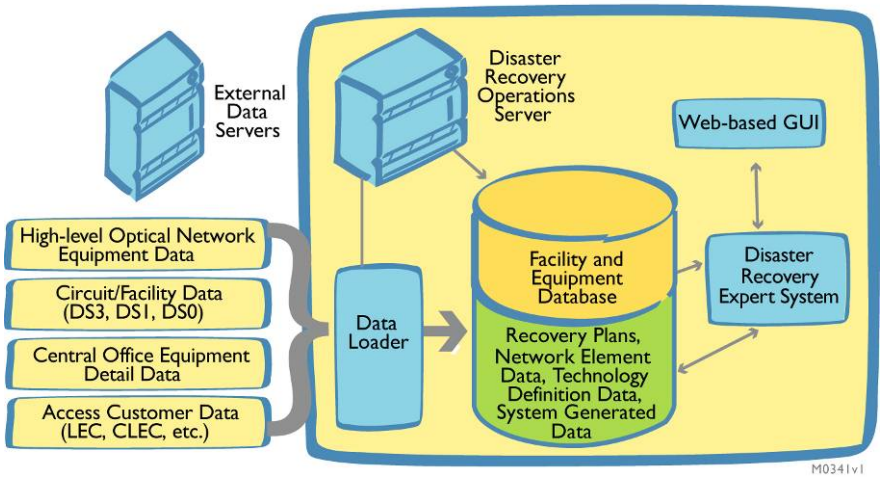


Figure 2.3.4-1: AT&T Disaster Engineering Connect Technology (DECT) High-Level Architecture. *AT&T draws on many resources to supply essential data and information for recovery efforts.*

The heart of AT&T DECT is a system that accepts facility and network element information for the AT&T network from our databases. Combined with a recovery site plan (automatic or manual), this system recreates the failed Network Office by generating the specific inter- and intra-trailer connectivity based on existing rules of recovery and the available recovery network elements in the AT&T NDR trailers.

The Disaster Intelligent Recovery Engineering Connection Technology (DIRECT) and Local Network Services Technology Automated Recovery (LONESTAR) systems support the automated re-engineering of circuits and facilities. These systems provide DECT with an online inventory of available transport, Digital Cross-connect Switch (DCS) and voice switching systems (Lucent 4ESS, 5ESS and Nortel DMS), and allow DECT to create recovery plans for connecting systems and restoring facilities for any AT&T long distance or local office. Cable tags, run sheets, DCS script files, office facility/equipment statistics and recovery reports are some examples of the output generated by these systems that assist NDR in a Network Office recovery.

3.0 DISASTER RECOVERY COMMUNICATION

3.1 Major Failure Notification Process

AT&T uses the Command, Control, and Communication Process (3CP) in order to manage network anomalies. Network anomalies are defined per the individual network technologies according to how they might adversely impact customer network service.

The Emergency Response Plans (ERP), Disaster Recovery Plans (DRP), Major Failure Action Binder (MFAB), Major Incident Plan (MIP), and alert processes developed and documented by appropriate organizations fit under the 3CP umbrella. These instruments allow organizations to readily respond to emergency situations from network, human resources, safety, and security perspectives.

Per the 3CP process, personnel are notified by pager and/or called at work or home in the event a disaster is declared at an AT&T Network Operations Center. DR team members are notified by their Disaster Recovery team leader. All team members are briefed on the current status, and a DR conference bridge (as described below) is established to discuss activation of the written DR procedures.

3.2 AT&T Internal Communication

When a disaster occurs at an AT&T facility location (Network Office or Facility POP), the NDR Duty Officer and the key NDR managers assess the problem and determine if a DR team should be deployed. AT&T's internal communication within NDR and with key impacted stakeholders follows a tightly-controlled step-by-step plan that starts with the activation of a special NDR conference call. This always-available conference bridge, called the Management Control Bridge (MCB) is established. Authorized stakeholders have specific instructions about how to join the bridge and cascade

information to impacted organizations. The NDR Duty Officer calls/pages the other NDR stakeholders. They meet on the MCB and determine the appropriate response to the disaster. On this bridge, after discussions and information sharing, a decision is made to activate the NDR process. This activation sets in motion the actual site failover or deployment of specific NDR trailers. If the Duty Officer is not available to join the MCB, a designated back-up assumes that role. Continual status during the disaster recovery process is provided on the MCB.

To facilitate communication at the disaster site, Emergency Communications Vehicles (ECVs) are deployed. The ECVs are described in more detail in section 5.3.1 below. The ECVs are four-wheel drive vans equipped with the following:

- 2 generators
- Supplemental cooling and heating systems
- An auto-positioning 1.2m satellite antenna
- A Ku-band satellite modem
- Automatic leveling jacks.

The ECV is capable of supporting a mix of 96 voice/data channels and an Ethernet LAN connection within minutes of arriving on location. These ECVs provide the ability for on-site technicians to communicate with each other, within AT&T, with suppliers, and with emergency personnel. Communication is further supported with satellite telephones and two-way radios all powered from the ECV. All NDR team members are provided with Government Emergency Telecommunications Service (GETS) cards to allow them priority access on the network during a disaster.

3.3 Communication with the Government

The CPO provides notification to the PMO whenever a disaster occurs that impacts Networx services. For an event that has a major impact on services, this notification occurs within 15 minutes. Notification is given to the GSA program contact names provided (Section C.3.2.3.1.1) for the PMO, Contracting Officers Representative (COR) and customer service representatives. The contact names and their contact information are recorded, maintained, and are readily accessible in the CPO. Included are email addresses, primary and alternate phone numbers, including cell phone and pager numbers.

Our disaster recovery liaison officer, [redacted] coordinates with the PMO to establish a common situation overview and establish priorities for the response. In the event of a disaster, [redacted] continually interface with the NDR Team and PMO as the Disaster Recovery actions progress. AT&T keeps the PMO informed of the recovery status as well as an estimated time of service restoration when it is known, using the Government Emergency Telecommunications Service (GETS), if necessary.

3.4 Communication to Critical Government Locations

AT&T understands that communication requirements from AT&T's NOCs to National Communication System (NCS) locations or other critical Government locations during an emergency will be defined by the Government after contract award.

3.5 Communication with Suppliers, Partners, and Other Networx Stakeholders

3.5.1 Cingular

For wireless services, our team member, Cingular, implements its well-established Disaster Recovery plan. In the case of a disaster, a communication channel is set up between our Disaster Recovery Liaison Officer and Cingular's Duty Officer, to coordinate all activities.

Cingular maintains pre-programmed phones for emergency situations. These phones can be accessed 24X7 and shipped by air or ground within hours of receiving notice. Cingular maintains spare batteries and rapid battery charging units. In the event that wireless and wireline telephone services are impacted, satellite phones and two-way radios are in place for communication between field technicians and incident management groups.

Once notified, Cingular coordinates with the local market to get the necessary phone numbers, program the phones, and ship the phones directly from Cingular's inventory. An inventory of phones might be provided or allocated on-site for dedicated government units, regions, or sites.

Cingular Outage Notification Process

Based on predefined network performance levels, broadcast notifications for incidents/outages are provided to key field personnel via text message or voice mail, alerting designated Cingular employees to network incidents. This process ensures succeeding levels of management are engaged in restoration and communication activities. During a disaster, Cingular's crisis communications plan facilitates internal and external communication and helps ensure that open lines are maintained between Cingular and its customers.

Cingular Wireless Priority Service

In compliance with the Department of Homeland Security's National Communications System's Wireless Priority Service (WPS) program, Cingular currently supports Wireless Priority Service nationwide except for the Ohio Valley, which is scheduled to be deployed in 2006. WPS is the wireless complement to the wireline GETS, which utilizes the Public Switched Telephone Network (PSTN) to provide enhanced wireline priority service to qualified personnel. WPS users who meet the approval criteria are authorized and encouraged to use GETS to increase their probability of completing their call during periods of wireless and wireline network congestion. The qualifying personnel categories include the following:

- Executive leadership and policy makers
- Disaster Response/Military Command and Control
- Public health, safety and law enforcement command
- Public services/utilities and public welfare
- Disaster recovery.

These personnel categories were selected to meet the needs of the emergency response community and provide access for the command and control functions critical to management of and response to national security and emergency situations, particularly during the first 24 to 72 hours following an event.

3.5.2 Global Crossing

For non-domestic services, Global Crossing NOC staff immediately initiate their Disaster Recovery response process according to plan and according to the type of disaster. Concurrently, the designated Global Crossing Networx DR Officer contacts AT&T's program office using a prepared contact list. A communication channel, like the MCB described above, is set up between our

Disaster Recovery Liaison Officer and the Global Crossing's Duty Officer, to coordinate all activities.

3.5.3 Other Networx Stakeholders

Telenor's assigned DR Officer is contacted via their point of contact information to determine if mobile satellite services are required in the disaster recovery process. AT&T, together with the NCS National Coordination Center (NCC), works with affected Local Exchange Companies (LEC) during a disaster. AT&T's NCC representative works directly with the LEC NCC representatives to coordinate restoration activities. Telecommunications Services Priority (TSP) procedures are followed for access provisioning and restoration.

4.0 DISASTER RECOVERY STRATEGY

4.1 AT&T Strategy

AT&T's overall strategy is to be prepared *before* disaster strikes. Part of being prepared is assessing which operational locations are critical and what the impact would be on operations should they be lost. We prioritize these critical areas and assign levels of assurance to each. We then develop a primary and backup approach to restore services should the critical area(s) be lost, with a focus on three primary goals:

1. Route non-involved communications traffic around the affected area
2. Give the affected area communications access to the rest of the world
3. Restore communications service to normal as quickly as possible.

To accomplish NDR goals, AT&T has implemented highly reliable SONET rings, Intelligent Optical Network, high-tech tools such as Real Time Network Routing (RTNR) and [redacted]. The AT&T transport network uses the [redacted] system as one of its key tools to ensure

network reliability. First introduced in 1992, the [redacted] system instantly identifies fiber-optic cable failures on the core network and automatically begins rerouting circuits via spare capacity. Frequently, the [redacted] system restores 90 to 95 percent of service within two to three minutes. In the vast majority of cases, the customer is unaware there has been a problem.

A second part of our overall strategy is to assign highly skilled professionals to the tasks. By allocating the right talent, AT&T is able to uncover any critical deficiencies, keep abreast of technology, and develop new techniques and new equipment to improve our capabilities. The NDR Team is a mobile group of AT&T managers, engineers, and technicians that have received special training in the physical recovery of the AT&T network.

The final element in AT&T's strategy is to be fully prepared for a disaster by testing and practicing under the conditions AT&T would expect to encounter. AT&T's plan is supported by a full complement of specialized equipment and skilled personnel, who regularly test their plans, keep current on technology, and maintain the DR equipment so it is ready to go into action 24x7. Trailer trucks loaded with telecommunications equipment are ready for dispatch if a central office is destroyed. The trucks are strategically located across the country to allow us to quickly get to a disaster area regardless of where it occurs.

AT&T's recovery time objective (RTO) is to recover the lost functionality of a destroyed AT&T Network Office within 168 hours of activation by the AT&T GNOC, as listed in **Table 4.1-1**.

RECOVERY TIME OBJECTIVES (HOURS)	ACTIVITY
0	AT&T Global Network Operations Center (GNOC) activates Network Disaster Recovery
+12-24	NDR Trailers deployed from warehouse(s)
+36-72	NDR Team and NDR Trailers at staging location from warehouse(s)
+108-168	Trailers positioned and leveled at recovery site. Trailers splice into fiber optic cable that originally served the damaged Network Office. Office facility configurations replicated using AT&T DECT, LONESTAR or DIRECT
168	Service Recovered

Table 4.1-1: The AT&T Reaction Time Sequence. *Disaster Recovery performance is measured by the number of hours to achieve full restoration.*

After the NDR team is officially notified to deploy, personnel and equipment are targeted to be staged within 36 to 72 hours to begin recovery of the destroyed Network Office. During the next 48 to 72 hours, the NDR team assembles all of the equipment and recovers the service that normally passes through the destroyed building. During the subsequent 24 hours, the team works to recover the originating and terminating traffic that was in the destroyed building. The 168-hour RTO covers most Network Offices including the 4ESS switch locations. The actual recovery time achieved would be a factor of the distance from the nearest of the four geographically dispersed NDR warehouses around the United States and the size and complexity of the failed office.

The NDR team uses four primary recovery solutions (or strategies): mobile, static, hybrid, and vendor supported. Individual critical network elements are recovered as listed in **Table 4.1-2**. These are explained more fully below under Section 5.0, Disaster Recovery Capabilities.

CRITICAL NETWORK ELEMENT	AT&T RECOVERY STRATEGY
Backbone Transport Network	Mobile Recovery
Lucent Technologies 4ESS™	Switch Static Recovery
Lucent Technologies 5ESS®	Switch Mobile Recovery
ATM Switch	Mobile Recovery
Frame Relay Switch	Mobile Recovery
Local Network Services	Mobile Recovery
Nortel Networks DMS250/DMS500	Mobile Recovery

Table 4.1-2: AT&T Recovery Strategy for Critical Network Elements.

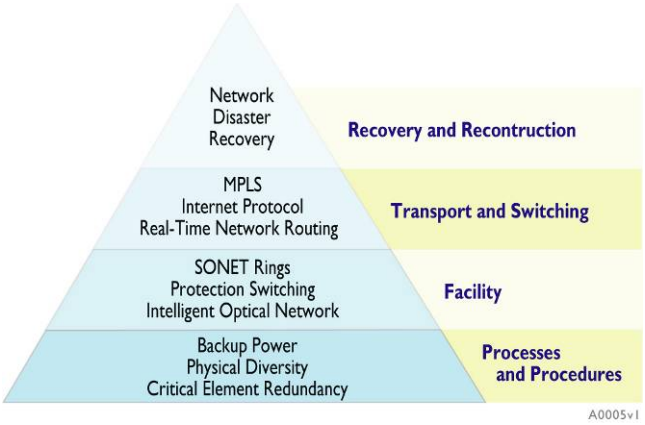


Figure 4.1-1: AT&T's Survivability Protocol. *A layered approach to disaster recovery helps to ensure that critical services are fully restored.*

For service delivering facilities, AT&T's strategy is to ensure continuity of service through network design and reliability principles, the layers of which are identified in AT&T's Survivability Protocol (refer to **Figure 4.1-1**). There are specific processes, tools and features that span the network to ensure that service is restored quickly and automatically in the event of an unavoidable service disruption.

At the first layer of the pyramid, *Processes and Procedures*, the network operations team uses a predictive, preventative and proactive (3Ps) approach. The basis of this philosophy is that the optimal approach to restoration is the ability to predict problems in advance and to build intelligent systems and alarms into the network (including rules and procedures to back them up). Failures are prevented or detected and corrected before service is affected. This includes proactive incident planning, such as in the instance of an impending natural disaster. For example, command and control is initiated prior to an anticipated incident occurrence to ensure a high-level of preparedness including topping off all fuel tanks, sandbagging locations where relevant, and proactively transferring to generator power before the storm hits to protect against any damaging event.

The second layer of the pyramid contains the automated systems, the physical layer, and the daily protection of the physical plant that transports calls and data traffic between AT&T offices. This includes SONET ring

restoration capability built into AT&T's core network architecture.[redacted], previously mentioned, is another example. In addition, our Outside Plant Protection practices are used at all times when work is performed around our buried facilities.

The third layer of the pyramid provides the intelligence of the network and its applications with various systems that support redundancy. This is primarily accomplished through network architecture and routing methodologies. By ensuring that single points of failure in the network (both at a component level and design level) are eliminated, the networks can be self healing in that they can detect failures or impairments and automatically switch to backup or redundant systems. Examples of these are routing protocols and Alternate Signaling Transport Network.

Even with controlled planning, maintenance, and architecture design, infrastructure outages can be minimized but failure risk cannot be completely eliminated. Hence, some failure factor can be expected which can only be mitigated through disaster recovery.

To affect disaster recovery in these cases, AT&T performs back-ups of operational support systems/data at a platform and system specific level, based on network components' individual architectures, hardware, operating systems and applications. These back-ups, however, must adhere to AT&T's DR standards to ensure continuity of operations. For critical applications, back-ups are always stored at an off-site location.

AT&T's Disaster Recovery program is capable of handling everything from network infrastructure to applications and security. Our strategy is to restore the network and all of the associated services riding on that network or supported by that network. This can include:

- Call Centers / Work Centers
- Mainframes
- Open Systems - Unix, Linux, & Windows
- Storage Systems
- PCs/LANs
- Hot Sites/Warm Sites

The strategy for service restoration which includes prioritization and partial or full restoration is based upon the following service characteristics for business criticality and essential functions:

- Mission Critical – Any element that can directly bring down or effect call processing/data transport.
- Business Mission Critical – Direct and immediate customer service impact.
- Data Sensitivity – Content of the data within the application; and
- Application Criticality – Supported Business Functionality.

These factors are used to classify and prioritize the risks. These risk classification guidelines help us determine the criticality of a system or network. When considering possible threats against our assets, these are the expected outcomes that we guard against by deploying safeguards and countermeasures.

The risks are classified into four areas: Critical, High, Medium and Low.

Critical Risks are defined as any loss of a single asset or functionality that by itself will have an impact on the integrity of AT&T Core Business or impact to U.S. Government Operations. Examples include:

- Major outage immediately affects the business of our customers;
- Disruption of voice or data networks; and
- Disclosure of government data.

High Risks are defined as any loss of a single asset by itself that will cause major impact to deliver service to a customer or subset of customers. The loss of a single element or component will impair AT&T's ability to provide core business functionality. Examples include:

- Disruption or impairment to AT&T's Network maintenance, provisioning, or surveillance capabilities;
- Disclosure or change of critical customer data;
- Disclosure or change of Corporate Proprietary Data;
- Inability to deliver services to customer; and
- Impacts to multiple interfacing assets.

Medium Risks are defined as a loss that could impair the functionality of the core business or ability to deliver some services to the customer. Examples include:

- Loss of some but not all functionality or service;
- Assets that have workarounds for period of time;
- Affects less sensitive and critical assets; and
- Data collection systems (if data sensitivity mitigated).

Low Risks are defined as a loss of an asset or disclosure of information that has little or no impact to AT&T or its customers. Examples include:

- Public information; and
- Non-critical systems/assets.

Knowing that disasters take many forms and can hit suddenly with little or no warning, AT&T reacts to ensure customer restoration.

In addition, AT&T works directly with Agencies to custom engineer a Disaster Recovery Plan for their Management and Applications services and Security services. Each program is custom designed based on Agency specifications.

Every AT&T facility has a Disaster Recovery plan that includes facility, personnel and assets needed to support the services AT&T provides. . Since the merger of SBC and AT&T, we have embarked on a comprehensive review, enhancement, and exercise plan for Business Continuity operations throughout the merged company. These activities embrace every aspect of business continuity for the new AT&T and all of our customers, to ensure standardized but tailored processes for every system, every application, every facility and every employee.

Further specific detail on Disaster Recovery plans for restoration and prioritization of Security services is provided in Section 5.2.

4.2 Cingular Strategy

For a disaster affecting wireless services, AT&T is in continual contact with Cingular, who launches its fully implemented and successfully demonstrated disaster recovery program.

Cingular's wireless network is designed to be reliable, survivable, and recoverable. Wireless cell sites and switching facilities are built to meet or exceed regulatory standards. Cingular designs extensive redundancy, including duplication of vital hardware, into its Mobile Switching Centers (MSCs) and other critical network nodes. The MSCs are equipped with automatic alarm notification systems for fires, extreme temperatures, and intrusions. If damage does occur, this flexible network is able to be reconfigured to bypass damaged equipment.

Cingular purchases the highest quality equipment and installs it in required or practical areas. The larger markets have multiple Mobile Telephone Switching Offices (MTSOs) and regional Network Operation Centers (NOCs) in different locations. If there is a disaster, transmissions are routed to the undamaged MTSO or to the NOC, based on the nature and location of the disaster and traffic type (communications or management). In case of large outages, emergency generators are ready to be dispatched and all locations have backup batteries. In addition, Cingular can employ alternate routing, its own private network, and leased high-capacity networks, if needed.

Cingular's Wireless Network Control Center plays a key role in detecting an incident, determining its severity, and initiating the appropriate notification and escalation processes. Duty officers (and backup duty officers) are obtained from Operations Support, each Field Service Area, and other critical business units on a pre-assigned 24X7 basis.

On a day-to-day basis, outages are managed using three levels of conference bridges. This includes a Cingular working bridge for the technical team and two separate bridges for escalation. The severity and duration of an outage determines escalation intervals. Network elements are monitored over time and escalated when an outage reaches a designated time threshold.

Subsequent increases in either the impact or length of the incident will initiate the appropriate escalation.

4.3 Global Crossing Strategy

Global Crossing provides business continuity and a Disaster Recovery Plan as part of its System Emergency Response Plan, which is an element of its overall security plans and procedures. These procedures are tested annually to ensure the System Emergency Response plan is current and effective.

When serving as a subcontractor, Global Crossing participates actively in the prime contractor's continuity of operations planning and teams, providing effective disaster recovery plans for all network operations under their control, and managing disaster recovery from their two central system-wide NOCs located outside of [redacted]

As listed in **Table 4.3-1**, Global Crossing defines three levels of disaster and regards any outage or degradation of service as an emergency.

LEVEL	EXTENT OF DAMAGE	EXAMPLES OF CAUSES
1	Local, well-defined outage or degradation of service occurring at a specific facility	• Damaged or cut LEC circuit(s) • SDP component failure • Local fire, flood from storm, or power failure that affects the backup generators • Localized malicious attack on the facility
2	Broader area, regional outage due to natural disasters or regional disruption	• Hurricane, earthquake, or other regional natural disaster • Assault on a primary POP or Switch Node within the network • Damaged or cut backbone fiber
3	Infrastructure assault, placing the entire network at risk	• National emergency • Malicious assault on the entire network (e.g., major denial of service assault) • Fire, flood, or assault on the NOC

Table 4.3-1: The Global Crossing Team Ranks Disasters. *Disasters are classified so that resources can be deployed as advantageously as possible.*

If a disaster occurs, the NOC staff immediately initiates response process steps as listed in **Table 4.3-2**.

GLOBAL CROSSING DISASTER RECOVERY PROCESS STEPS

Step	*Description*
1	The Help Desk staff or the NOC initiates a trouble ticket
2	The damage is assessed and the location(s) isolated
3	Testing is done to further determine the nature and extent of the damage
4	Recovery plans for the type of damage are initiated
5	If the problem is within the backbone or a POP, the Global Crossing NOCs are notified and mobilized

6	The local access provider is notified if the problem is within the "last mile" connection.

Table 4.3-2: Global Crossing DR process. *Risk to Government customer is minimized by adherence to a pre-defined process.*

4.4 Telenor Satellite Services

Satellite communications itself serves as the backup for disasters occurring to the landline and wireless services, sometimes being the only restoration option available. The key requirement is a direct line-of-site to the sky. Telenor Satellite Service, our mobile satellite service provider, delivers its services on Inmarsat, Iridium, Thuraya and Globalstar. In the unlikely event that one of these satellite constellations, or the fixed satellite services, would be put out of commission, service reverts to another one for either voice or data services.

5.0 DISASTER RECOVERY CAPABILITIES

Prior to the attack on the World Trade Center on September 11, 2001, AT&T's NDR Team had never called for a full-scale deployment. Today, with the NDR's mobile capability, our objective is to replace a totally destroyed Network Office and completely restore service within 168 hours.

> *"AT&T not only is the patriarch of today's disaster recovery programs, it is also the kingfish. AT&T has spent more than $300 million on the effort since 1991, and much of that money has been spent on 20-foot semi-tractor trailers that house network equipment capable of replicating any domestic or international transport scenario. Four times a year, once in each region, AT&T rolls the trucks and conducts disaster simulations."*
>
> --Telephony, August 2003

The three major disaster recovery descriptions included in the attachments to this DR Plan are the best evidence of AT&T's disaster recovery capabilities. Each one demonstrates different capabilities required to meet the challenges of both natural and man-made disasters (Attachments A-C.) In addition, NDR has dispatched its equipment and team in response to smaller scale problems affecting the AT&T Network. Those partial and precautionary deployments included responses to fires, flooding, an earthquake, a gas line

explosion, and a train derailment. The NDR Team has also provided emergency communications support for a variety of humanitarian relief efforts. To accomplish Disaster Recovery AT&T relies on a combination of tools, skilled personnel, specially designed equipment, and effective testing.

Recovery tools

AT&T relies on automated tools, such as Real Time Network Routing (RTNR) and [redacted] has the capability of rerouting circuits within 60 milliseconds of a failure on the core network. With this kind of response to network failures, the GSA and subscribing Agencies may not even detect service disruption.

Skilled Personnel

The composition and caliber of the personnel making up our NDR Team has been discussed in Section 1.0 above. Their capabilities are kept current by regular exercises.

Mobile Equipment

In order to restore Government and commercial communications as quickly as possible following a disaster, AT&T maintains a fleet of specially-designed trailers and equipment staffed with a team of highly-trained professionals on call 24x7. Their goal is to restore functionality within 168 hours of being activated.

All of the telecommunications equipment required to recover a destroyed AT&T Network Office is transported to the site in these technology trailers. Each trailer has self-contained power and environmental capabilities and each houses a component of the network technology that would normally be part of a permanent installation.

Figure 5.0.3-1: AT&T's Response to World Trade Center Disaster. *Equipment and personnel can be en route to an emergency incident within two hours of an official call-out.*

Team members and equipment can be en route to an emergency incident within two hours of an official call-out. In the case of a forecasted disaster, such as a hurricane, they are often dispatched to strategic locations prior to the event. The specially-designed tractor-trailers, (**Figure 5.0.3-1**) equipped with highly sophisticated equipment, generally travel by road, but in an extreme emergency can ship by rail or air.

A more detailed description about our mobile equipment is included in Technical and Operational Capabilities.

5.1 Management Capabilities

AT&T, as lead in the Networx program, is responsible for the coordination of subcontractor service delivery, both domestic and non-domestic. AT&T's Disaster Recovery Team works closely with our suppliers of access, equipment, and other necessary products and services to prepare, implement, and modify their Disaster Recovery plans to ensure they meet our needs for replacement services and equipment in the event of a disaster. These plans, policies, procedures, and supply channels are tested annually and have been refined over years of working together. This experience also helps us plan with our suppliers and partners, the amount of spare equipment needed in storage and what geographical locations are best suited for quick deployment. In addition, AT&T provides conditioned open bay space in our Disaster Recovery Trailers for local providers to mount equipment and

terminate their service to facilitate service restoration. AT&T has reviewed the disaster recovery plans and strategies of our subcontractors as part of the partner selection process, and verified their plans to be acceptable. AT&T will continue to monitor their DR practices with annual tests and evaluations, reporting our results to the Government throughout the life of the program.

For service restoration including prioritization and partial or full restoration, AT&T uses TSP (Telecommunications Service Priority) guidelines. Customers who utilize this service are generally qualified for the treatment and have a need for “essential service”. Government customers, police and fire, disaster aid, hospitals and others are among the customers that use this service. When restoration efforts are required the GNOC prioritizes the order of work to be performed at a network component level. AT&T has restoration capabilities using prioritization algorithms. One example is [redacted], a restoration capability used to automatically reroute transport capacity in the event of a service disruption. Every T1 circuit is assigned a score based on type of service (TSP, signaling, private line, message trunks). The scores are summed for all of the T1 circuits within the higher order circuit (T3), providing a score for the T3. The T3s with the highest prioritization score are automatically restored first by [redacted]. With [redacted], Agencies can be confident their service will be correctly prioritized for restoration.

The mission of the NDR Team is to restore AT&T communications to an affected area as quickly as possible. To accomplish its mission of rapid service restoration, NDR applies one of four solutions as shown in **Figure 5.1-1.**

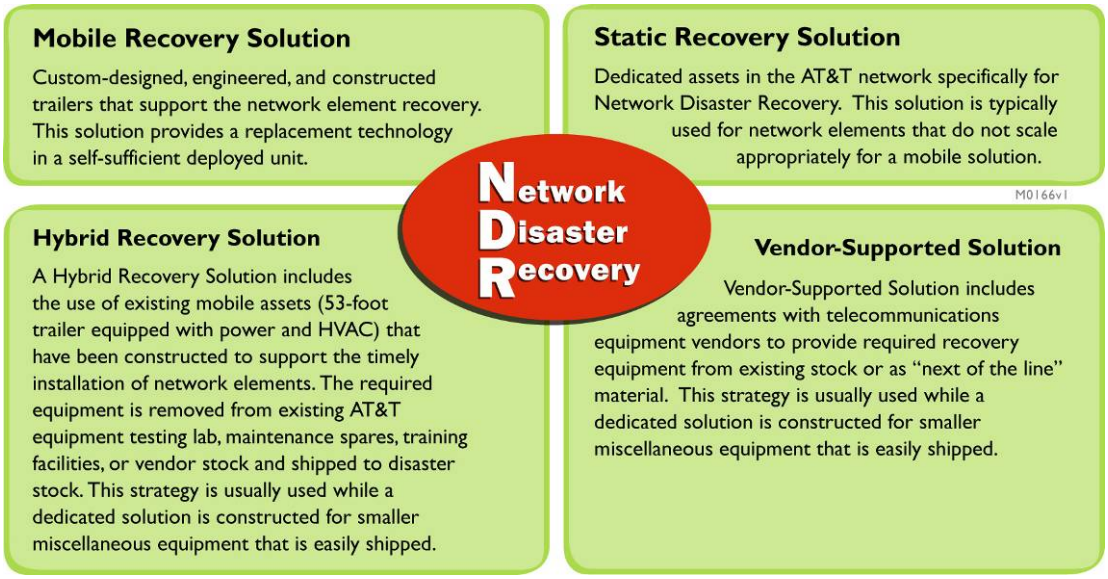


Figure 5.1-1: Network Disaster Recovery Solutions. *AT&T selects the appropriate solution before deploying.*

In addition to the NDR organization described above in Section 1.0, an Infrastructure Technical Services Group (ITSG) exists to assist in the initiation, coordination, restoration, and reconstitution of AT&T's telecommunications facilities under all conditions, crises or emergencies.

ITSG is responsible for providing Tier II and Tier III building infrastructure technical support for all infrastructure assets of AT&T: Domestic, International and Local. ITSG provides technical support for engineering, development and distribution of infrastructure bulletins, incident management, restoration of power/environmental equipment and the management of all aspects of programs within the Field and Center Technical Support (FACTS) Division.

Tier II and Tier III Building Infrastructure Technical Support:

- Provide 24X7 technical support and maintenance functions related to the infrastructure technologies
- Perform installation reviews of infrastructure assets implemented into the network

- Incident management for critical infrastructure, hurricanes and other disaster situations
- Provide Communication, Command and Control Process (3CP) support to the GNOC for disaster situations and resolution of network troubles related to the infrastructure technologies
- Perform technical office reviews for standard adherence and assist with maintenance routines
- Participate in national disaster exercises and deployment
- Physically respond as necessary to critical infrastructure/environmental and disaster situations.

5.2 Technical Capabilities

Backbone Transport Network Mobile Recovery

Figure 5.2-1 shows the configuration used for mobile recovery of the backbone transport network that supports the AT&T Network Services. The individual components are interconnected to match the unique configuration of a heavily damaged or destroyed Network Office.

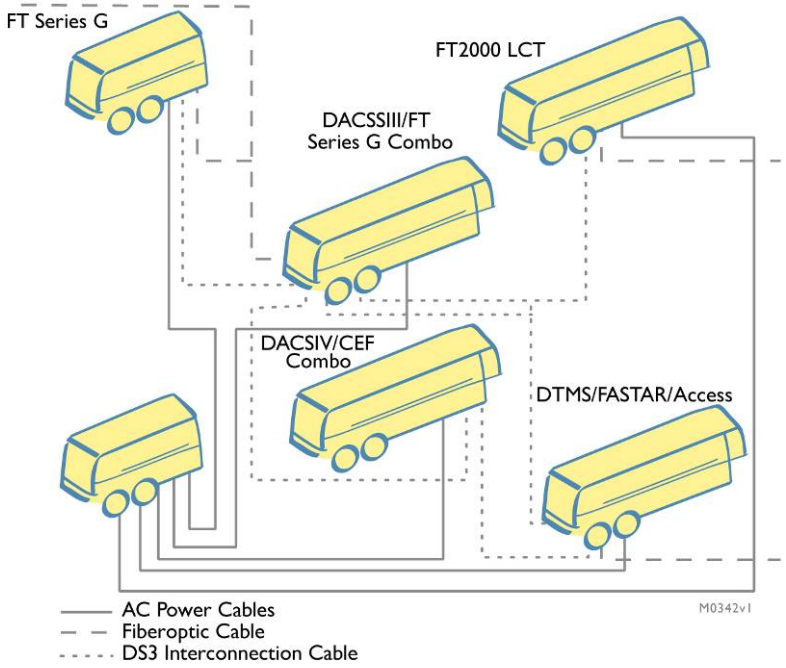


Figure 5.2-1: Backbone Network Disaster Recovery Configuration.
Interconnected mobile trailers provide the capability of a Network Office.

4ESS Switch Static Recovery

AT&T has a Lucent Technologies 4ESS™ switch in a hardened underground location in our network that is dedicated to Network Disaster Recovery. It can be configured to replace and assume the identity of any failed 4ESS™ in the AT&T Network. The combination of the trailer-mounted transport elements, dedicated spare T3 (T3R & T3P) facilities and this spare 4ESS™ switch allows for the recovery of an AT&T 4ESS™ switch office should a catastrophic event occur.

The Disaster Recovery process for the 4ESS™ switch has five key components:

- A centralized spare 4ESS™ switch maintained and connected to the network as a “live office” but with the capacity dedicated to Network Disaster Recovery
- Office data, which is electronically backed up at regular intervals to a remote location near the spare switch
- Processes/systems required to map data from failed elements to recovery elements
- Trailer-mounted Access/Egress equipment to replicate/recover elements in the failed location
- A highly skilled and motivated Network Disaster Recovery Implementation Team with representation from key operational organizations.

Figure 5.2-2 provides an example of this type of recovery solution.

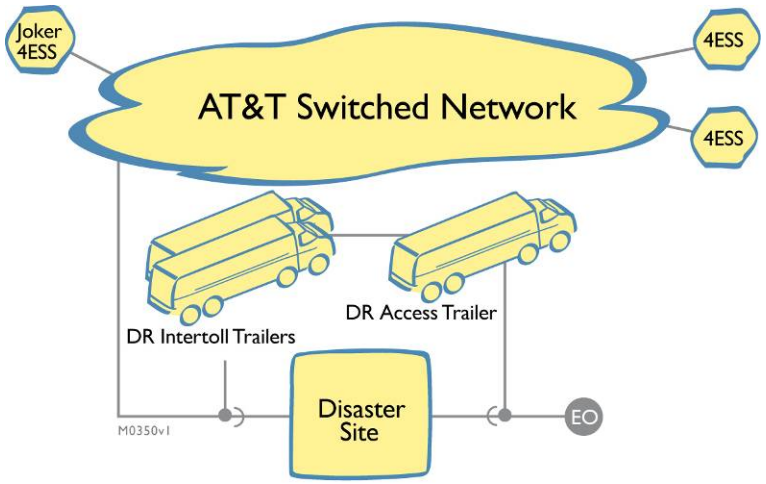


Figure 5.2-2: 4ESS Disaster Recovery Configuration. *Joker switch at hardened site aids recovery of damaged 4ESS™ switch office.*

5ESS Switch Mobile Recovery

AT&T has a 5ESS® Disaster Recovery three-trailer set utilizing a Lucent Technologies 5ESS 2000 switch core with seven Switch Module 2000 (SM2000) line/trunk growth units. This 5ESS Network Disaster Recovery trailer set is capable of recovering approximately 68,500 lines/trunks. AT&T has added a second 5ESS recovery trailer utilizing a Lucent Technologies 5ESS 2000 switch core and five Switch Module 2000 (SM2000) growth units capable of recovering approximately 63,000 line/trunks. Incorporating the new Communication Module Model 3 (CM3) technology, this 5ESS trailer maximizes the recovery capabilities within a single container. It also utilizes the latest packet signaling technologies, eliminating the previous ring node architecture.

ATM Switch Mobile Recovery

AT&T uses a trailer equipped with Lucent ATM switches. In their current configuration, the switches can handle circuits from T1 up to OC-12, with a net capacity equivalent to over 900 T3s. The trailer is pre-wired to nearly double this capacity with additional plug-ins and switches, **Figure 5.2-3**.

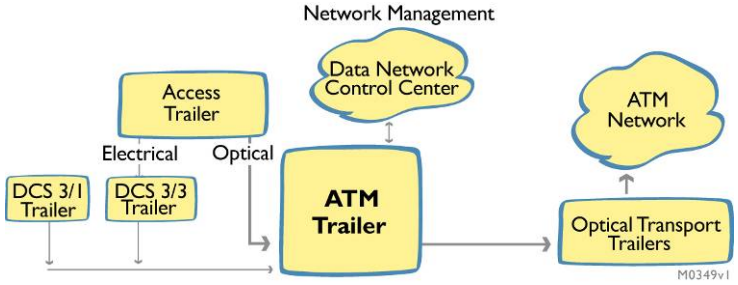


Figure 5.2-3: ATM Recovery Architecture. *ATM recovery provides net capacity of more than 900 T3 lines.*

Frame Relay Switch Mobile Recovery

In this solution, self-sufficient Frame Relay Switch trailers have two BPX 8620s and one MGX 8850. Each trailer has 16,128-DSO recovery capability. The trailers were first field-tested in the fourth quarter of 2000 at the NDR exercise in Phoenix, Arizona. (**Figure 5.2-4**)

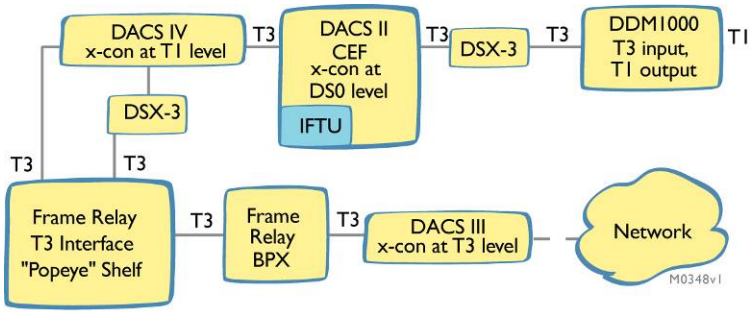


Figure 5.2-4: Frame Relay Recovery Architecture. *Depicted is the equipment in the data path utilizing FR and transport technology trailers. Note that for needed capacity more than one FR switch is connected.*

Local/Metro Network Services Mobile Recovery

AT&T has developed a Network Disaster Recovery capability for our Metro Network Services. Capabilities include switching and transport for DCS3/1, DCS 1/0, SONET Lightguide, and OC3/OC12/OC48/OC192 multiplexer network elements used by AT&T to provide local network services.

Figure 5.2-5 depicts AT&T NDR's mobile solution to support optical deployment of MSPs (Multi-Services Platform) that connect to AT&T's Dense Wavelength Division Multiplexing (DWDM) backbone network.

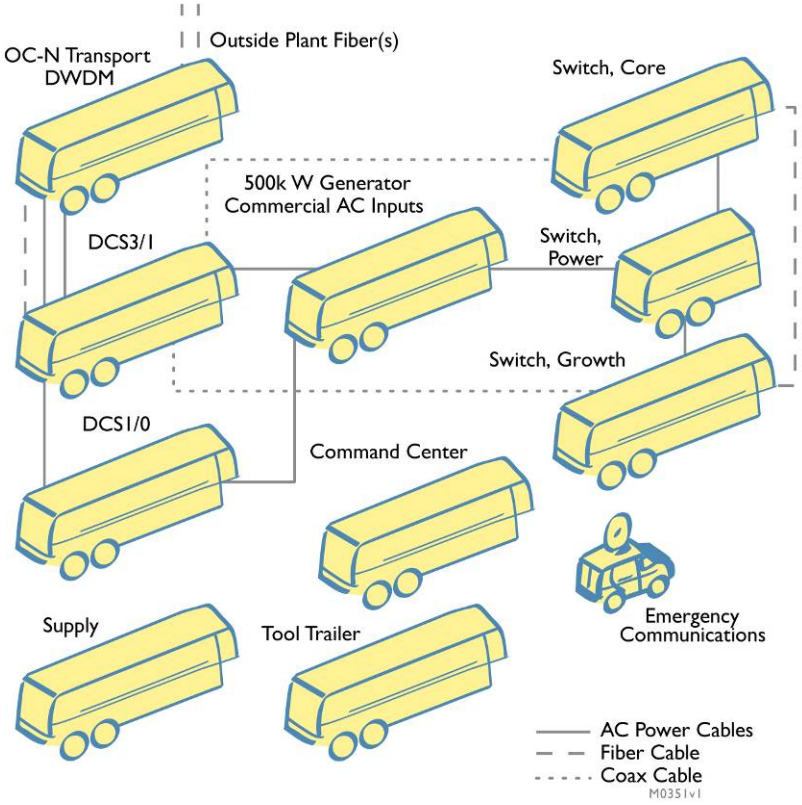


Figure 5.2-5: Local Network Services Recovery Trailer Plan. *NDR's mobile solution provides connectivity to AT&T's backbone network.*

DMS Switch Mobile Recovery

AT&T has a DMS500 Disaster Recovery trailer set utilizing a Nortel Networks DMS500 switch. This trailer set supports DMS500 and DMS250 switches for AT&T Long Distance and Local Services networks. The DMS trailer-mounted set using Spectrum Peripheral Modules can recover up to 56,000 line/trunks and Extended Subscriber Modules up to 240 DS1s.

IP Recovery

Figure 5.2-6 shows the IP Recovery trailer. It is packed with Cisco, Avici and Juniper routers with net switching capacity well into the terabit range (over 1000 Gigabits/second). When fully supplied with plug-ins, the trailer can scale up to more than 10,000 T3s of capacity and support recovery of circuits as large as OC-192. With a single trailer, NDR can recover thousands of circuits

at speeds up to 10Gbps. Working with AT&T Labs, NDR has developed a design that can recover the largest AT&T common backbone sites using half the number of routers.

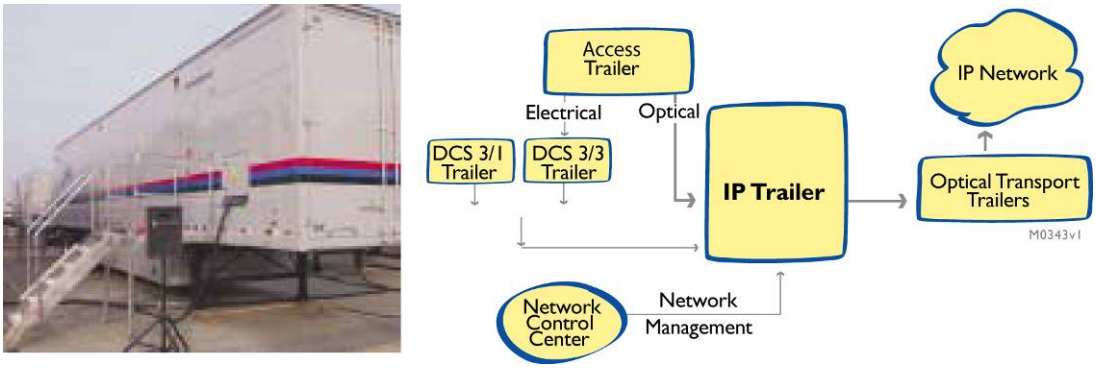


Figure 5.2-6: IP Trailer and Functional Architecture. *A single trailer can recover thousands of circuits at speeds up to 10Gbps.*

Intelligent Optical Network Recovery

The vision of end-to-end interconnectivity with fast and simple provisioning of customer circuits and capital cost savings are the primary motivators for the Intelligent Optical Network and the processes that support it. The intelligent optical network and its technology and operational benefits include a suite of Multi-Service Platform (MSP) sub-networks interconnected by the Intelligent Optical Switch (IOS) mesh transport network. Key benefits of this technology are fast provisioning via “point and click” and improved restoration performance via IOS mesh restoration—all while meeting business objectives.

NDR has constructed a mobile solution in the event of a catastrophic Common Network Interface (CNI) office failure. NDR will be able to recover offices with the Core Director IOS, shown in **Figure 5.2-7** and offices with MSPs for both long distance and local service applications.

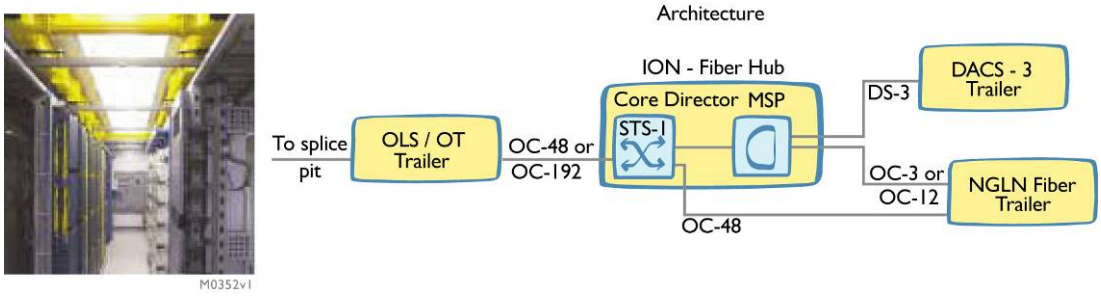


Figure 5.2-7: Intelligent Optical Network Architecture. *This mobile solution will restore offices providing long distance and local service.*

AT&T Global Network (AGN) Recovery

NDR has developed two sets of disaster recovery containers to support AT&T Global Network Tier 1, 2 and 3 POPs for our globally deployed services. These containers use Cisco routers, ATM switches, Catalyst switches, GIG-E switches, MSP interfaces, and a CI IOS switch. AT&T has an AGN presence in over 130 cities worldwide with a total of 146 nodes in 130 cities. Together with our "Fly-In" recovery containers, staged in Europe and the United States, AT&T can support the recovery of in-country AGN architecture.

In a disaster, AT&T would bring these “fly-In” containers to an airport for transportation to the affected country. The Global NDR team supports the logistics for deployment, connection and shipping when a transition to an in-country team is planned to maintain the container set in production. The team utilizes military-style aluminum containers (sized to fit inside a standard 747 or any wide-bodied freight carrier) that are supported by both in-country and/or generator power and designed to operate under a wide range of voltage inputs.

One set of the containers for Europe, Middle East, and Africa (EMEA) is staged in the United Kingdom (UK) at a specially built staging station, with the second in one of the NDR warehouses in the U.S. The containers staged outside the U.S are permanently connected to the AT&T Global Network to receive IOS upgrades and are monitored and managed by the Global

Network Operations centers in the US. The two sets on either side of the Atlantic mirror each other in technology and capability. They represent a unique recovery strategy in most-of-the-world (MoW, i.e., non-US Countries) and a significant investment in support of ours and our customers' global strategic network architecture. (**Figure 5.2-8**)

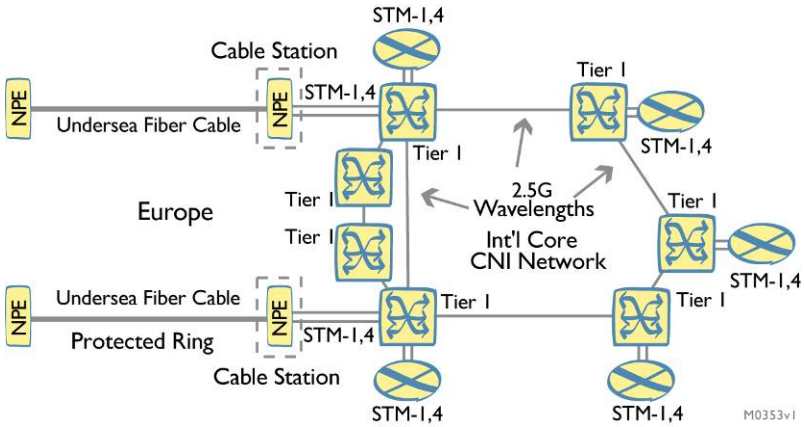


Figure 5.2-8: AGN Network – EMEA. *AT&T mobile solutions can be hauled or flown in to restore global network locations overseas.*

Recovery of OSS Applications

In the event of a disruption in computer operations, GSA and Agencies can be assured disaster recovery plans are in place to provide continuity of all parts of the network and the services riding on it, including OSS, all Management and Applications services systems and all Security services systems. These disaster recovery plans include routine steps to ensure preparedness, such as regularly scheduled software backups and management of backup media. Recent software and data backups would be essential if it became necessary to recover from a disaster, whether a natural disaster, such as a fire or flood; a crime, such as an intruder's vandalism of the network or a supporting computer facility; or a hardware or software failure or user error. Duplicate backup media must be stored off site to minimize the risk of being damaged or destroyed with the production environment.

To provide this safeguard for the Government, backup files are created on a prescribed schedule and rotated off-site often enough to avoid disruption if

current files are damaged. Alternate storage site(s) will be geographically removed from the primary site(s) and physically protected at the same level that the primary site(s) is protected.

If there is an alternate processing site, GSA and the Agencies are notified through a contract or interagency agreement to ensure availability of the alternate site.

The **Business**Direct portal to the OSS applications is available from multiple active servers in geographically separate locations. The entire production platform is replicated at a second site for Disaster Recovery fail-over. The second site is an exact hardware duplicate of the primary, and is kept synchronized with the primary site in the following areas:

- Platform and application software
- Server configuration files and data
- Application data.

The OSS applications are also hosted on servers with an alternative server in a geographically removed secondary site. Critical OSS applications are restarted on the appropriate alternate server by the AT&T OSS management organizations, and the data is restored from backup.

Recovery of Security Services

AT&T's approach to Disaster Recovery addresses architecting disaster recovery into the fabric of the Security services as well as the common infrastructure that support these services. In order to better understand the nature of disaster recovery as applied to Security services, further technical capability detail is provided as it relates to AT&T's Managed Security Services (MSS) offering. MSS at AT&T are offered under two major scenarios: 1) Customer Premise Solutions (CPS) and 2) Shared Solutions

(SS). Customer Premise Solutions are offered in two flavors: 1) Solutions on the actual customer premise and 2) Solutions that exist on AT&T real estate. Shared Solutions are services offered on common security equipment which customers share in a virtual secure space.

Customer Premise Solutions

AT&T offers managed security solutions in the CPS space, such as managed firewall service or intrusion detection and prevention service. These services are architected to meet the various needs of customers in the availability spectrum (DR). For Networx, these services are offered in configurations that meet or exceed the acceptable quality levels defined for the key performance indicators. AT&T can provide these services in configurations that offer high availability both on a local and remote basis. Customer Premise Solutions allows the customer to configure a solution that best fits their business requirements. The status of these Customer Premise Solutions is monitored continuously and on-site support is provided within the period specified by the acceptable quality levels. When these Managed Security Solutions reside in AT&T's hosting facilities, AT&T is responsible for the reliability and availability of the infrastructure. AT&T's hosting centers are architected with high availability in mind. These centers all have redundant communications, power and can withstand various physical threats such as high winds and flooding to name a few.

Shared Solutions

Shared security solutions are solutions that reside both within AT&T facilities and on common shared security platforms. The AT&T facilities are generally the Hosting facilities and/or the Service Node Routing Complex depending on the specific security function. Since this is a common shared platform each platform is architected with both local and remote high availability

configurations. For example our Network Based Firewall platforms exist in various hosting centers throughout the world. These platforms each have local redundant platforms within the hosting center as well as remote redundant sister platforms as a distant hosting facility. This architecture insures high availability in the advent of either a local or defined geographic disaster.

In addition to each of the shared security solutions having these types of high availability as part of the fabric of the service, these services once again are resident in AT&T's facilities which are also architected with high availability in mind.

Customer Prioritization

Customer prioritization follows the risk categories described in section 4 above. In addition, Customers are able to customize the level of availability solutions and SLAs that meet their needs.

5.3 Operational Capabilities

Recovery efforts during a disaster are supported by the operational equipment described below.

Emergency Communications Vehicle

Figure 5.3-1: An Emergency Communication Vehicle (ECV) at the World Trade Center Police command center in September 2001. *ECVs bring voice/data service up within minutes of arriving on scene.*

The AT&T Emergency Communications Vehicle (ECV) (**Figure 5.3-1**) is a four-wheel drive van equipped with two generators, supplemental cooling/heating, an auto-positioning 1.2m satellite antenna, a Ku-Band satellite modem, and automatic leveling jacks. The ECV is capable of supporting a mix of 96 voice/data channels and an Ethernet LAN that provide voice and data connectivity within minutes of arriving on location.

Light wave trailers convert local electronic signals to optical signals for transmission over AT&T's fiber optic, light guide network.

Portable radio towers are used to establish microwave repeater or terminal sites for locations where cable cannot be used.

Regen Trailers amplify or regenerate light guide signals.

Access Trailers provide points where access vendors can connect their equipment to the AT&T Network.

A **Common Network Interface Hub** utilizes mesh architecture to manage transport technology cross-connects.

Digital Access Cross-Connect Systems (DACS) trailers provide a junction point for telecommunications signals. The DACS trailers are used for signal grooming and interface to the optical systems that transport the service into the network.

Digital Radio trailers contain all of the equipment needed to recover a digital radio site.

DTMS/[redacted] trailers provide a satellite link from a recovery site to the AT&T Network Operations Center to allow remote testing. These trailers also support the [redacted] system to allow optimum routing of service through the site.

5.4 Cingular Capabilities

Cingular can deploy a mobile Cell-On-Wheels (COW) site consisting of base station radios, on-board power generation, a tower structure, and antennas, to replace or augment wireless services at any location where service has been lost or requires enhancement. A COW provides up to 40 channels when no other service is available. If wireless and wireline services are impacted, satellite phones and two-way radios are used for communication between field technicians and incident management groups. For such an emergency,

Cingular also maintains pre-programmed phones, including spare batteries and rapid battery-charging units, which can be promptly dispatched by air or ground.

Cingular's emergency/disaster preparedness program emphasizes prevention as well as recovery. Cingular has used this program to actively support events such as Y2K, the NATO 50, the Pentagon relief efforts after the September 11, 2001 attack, the Washington, DC mail anthrax incidents, and crisis management communications at the 2002 Winter Olympics. The Appendix to this plan offers other specific examples, including the Oklahoma City Federal building bombing, Hurricane Ivan, Hurricane Charley, and the 2003 California wildfires.

To ensure effectiveness during a crisis, Cingular also provides extensive disaster recovery training for employees and conducts regularly scheduled disaster exercises. These exercises employ realistic scenarios in which engineers and technicians identify and repair simulated damage resulting from possible disasters.

5.5 Global Crossing Capabilities

Global Crossing has protective design features in place such as:

- Span and protection ring switching with automatic rerouting
- Redundant and meshed core service networks
- Deployment of redundant power in all POPs
- Redundant switching and power equipment in all POPs and diverse routing of customer circuits.

Their disaster recovery capabilities include: hot site re-direction to a customer's disaster recovery center, a private line fan out service, service level back-up options utilizing a different product or platform, and ad-hoc conferencing services.

Global Crossing employs “self-healing” infrastructure technology such as: fiber protection, SONET redundancy, NOC redundancy, and router/switch redundancy to achieve network service continuity. They also have multiple Network Operations Centers worldwide, which are responsible for supporting customers on a global level and are accountable for service inquiries, maintenance, and trouble resolution, while providing regional support to ensure 24X7 coverage and local working knowledge. In addition, all NOCs use common methods/procedures, systems and tools, each NOC is backed up, and multiple remote access capabilities are available from multiple centers to all network elements.

Global Crossing maintains its preparedness through the continual training of personnel and by evolving with its customers’ emergency requirements, developing and offering options to meet their needs. An example is Global Crossing’s Diversity, Avoidance & Customer Specified Routing (DACSR), which provides a solution for two broadband circuits to be diverse from one another. The customer may avoid certain indicated routes and or particular Global Crossing POPs, and instead specify a specific route for their broadband circuit.

5.6 Summary of Recent AT&T Recovery Deployments

Over the past ten years AT&T has deployed its NDR more than a dozen times. Each event required deployments of different types of technology trailers to restore service. Because AT&T has mobile units designed for the replacement of all components in a Network Office, service restoration can be accomplished quickly no matter which type of catastrophic event has

occurred or which Network service was affected. **Table 5.6-1** outlines some deployments in recent events.

DATE	EVENT	LOCATION	EQUIPMENT
8/29/05	Hurricane Katrina	Gulf Coast	AT&T deployed Network Disaster Recovery trailers and extensive "power management" capabilities to appropriate sites and two Emergency Communications Vehicles (ECV) in the impact zone.
10/03	Wildfires	San Diego, CA	Technology trailers and ECVs to staging location near San Diego and held in reserve. ECV used for humanitarian relief.
9/02	Regenerator Damage	Hamilton Square, NJ	Regenerator Trailer to recovery site and held in reserve.
09/01 & 10/01	WTC Disaster	New York, NY	Technology Trailers and ECV to recovery site in New Jersey. ECV for humanitarian relief in Manhattan.
5/01	Tropical Storm Allison	Houston, TX	Limited trailer deployment, Subject Matter Experts, and ECV (emergency communications and humanitarian relief)

Table 5.6-1: Network Disaster Recovery Recent Deployments. *AT&T has the technical capabilities and a highly-skilled staff to respond to and restore catastrophic service outages quickly.*

AT&T's disaster recovery services are capable of responding to natural or man-made events ranging from attacks in cyber space to physical devastation. Examples of effective AT&T disaster recovery activities include:

- Hurricane Katrina (September 2005)
  - DHS/FEMA - Installed 137 T1s (3228 voice trunks) into call centers (North Hollywood and Dallas) in 5 days to provide critical victim support functions

> *Within 48 hours of Hurricane Katrina's landfall in New Orleans and the Gulf Coast, telecommunications contractors were on the ground, assessing damage to government facilities and identifying affected services. AT&T Government Solutions had more than 250 priority orders -- a huge number -- from government clients and first responders for circuit orders, said Lou Addeo, president of AT&T's government unit. The company also dispatched emergency communications vehicles to Louisiana and Mississippi for use by the state police, National Guard and for the airport and bus terminals in New Orleans, Addeo said. "Before the hurricane, we had these emergency vehicles located in the South ready to go," he said. "We put our assets where they need to go in times like this."*
>
> Washington Technology, online, 9/25

- Code Red Worm (July/August 2001)
  - More than 150 consecutive hours of coverage and 7,000 person hours were expended to identify and successfully implement fixes.
- September 11, 2001

- AT&T completed 431 million voice calls, surpassing the previous single-day record of 330 million calls, while responding to the communications needs of affected businesses with NDR teams and fully equipped tractor trailers

6.0 DISASTER RECOVERY READINESS/PREPAREDNESS

Readiness and preparedness for disaster is the core purpose of NDR's existence. Disaster Recovery readiness has evolved substantially since September 11. **Figure 6.0-1** encapsulates how our capabilities have shifted from being solely reactive to the modes of prevention and preparedness. This strategy has led to development of a stronger and more resilient communications infrastructure and better network diversity solutions and management tools, such as:

- Upgraded tools such as [redacted] that can automatically re-route damaged circuits after sensing an outage within 60 milliseconds.
- New CNI Hub and IP technology trailers to replace data network services for a destroyed Network Office.
- Ultravailable services are currently available and being implemented for customers with critical service requirements.

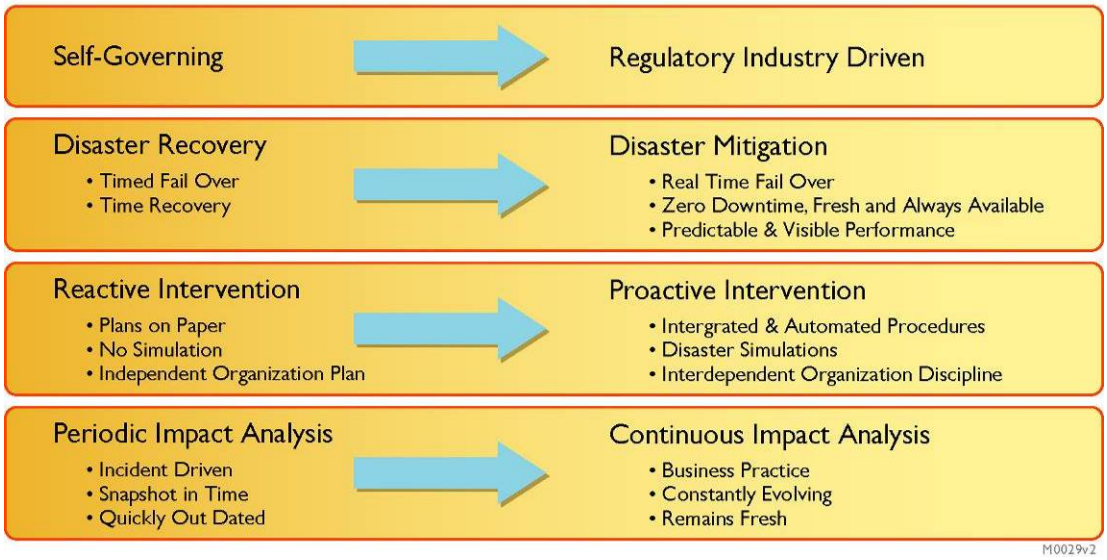


Figure 6.0-1: Shifting Paradigms: Zero Application Downtime. *AT&T Disaster Recovery adds prevention and preparedness capabilities.*

6.1 Annual Preparedness Drills

To further assure the Government of AT&T's readiness to offer the best disaster recovery capability available in the telecommunications market, AT&T requires disaster recovery plans to be exercised at a minimum annually, covering all assets, applications and network services. NDR has "exercised" its team members, equipment and processes in full-scale disaster recovery exercises held around the United States since 1993. These drills test as many of the NDR functions as possible, from the initial call-out, to equipment transportation and setup, to technology turn-up and testing. These exercises include simulation of failure conditions and recovery to either the DR location or platform. For network infrastructure, field exercises are conducted three to four times a year.

As illustrated in **Table 6.1-1**, AT&T's full-scale disaster recovery exercises were performed in various locations.

2006 EXERCISES

First Quarter	Dallas, TX
Second Quarter	Las Vegas, NV
Third Quarter	Washington, DC

Fourth Quarter		Miami, FL
	2005 EXERCISES	
First Quarter		Houston, TX
Second Quarter		Bedminster, NJ
Third Quarter		Kansas City, MO
Fourth Quarter		Atlanta, GA
	2004 EXERCISES	
First Quarter		Seattle, Washington
Second Quarter		Pompano Beach, Florida
Third Quarter		Foster City, California
Fourth Quarter		Saint Paul, Minnesota
	2003 EXERCISES	
Second Quarter		Chicago, Illinois
Third Quarter		Training Exercise
Third Quarter		Boston, Massachusetts
Fourth Quarter		Dallas, Texas
	2002 EXERCISES	
First Quarter		Training Exercise
Second Quarter		Ashburn, Virginia
Third Quarter		Training Exercise
Fourth Quarter		Bedminster, New Jersey
	2001 EXERCISES	
First Quarter		Training Exercise
Second Quarter		Tampa, Florida
Third Quarter		Denver, Colorado
Fourth Quarter		Canceled (WTC Deployment)
	2000 EXERCISES	
First Quarter		Training Exercise
Second Quarter		St. Louis, Missouri
Third Quarter		White Plains, New York
Fourth Quarter		Phoenix, Arizona
	1999 EXERCISES	
First Quarter		Training Exercise
Second Quarter		San Antonio, Texas
Third Quarter		Lodi, California
	1998 EXERCISES	
First Quarter		Salt Lake City, Utah

Table 6.1-1: DR Drills Instill Readiness. *Held in varying locations, readiness is reinforced through a simulation of catastrophic events.*

Upon completion of each disaster recovery exercise, a grade is assigned, based on an evaluation of its recovery preparedness utilizing AT&T's Certification and Assurance standards. The objective is for mission-critical plans to achieve a B or better certification grade. The results form input into the annual Disaster Recovery Plan updates.

AT&T routing and disaster recovery services, coupled with 24/7 tiered support within the operation, is a huge selling point for us. Being able to rely on them and never second- guess their decisions allows us to sleep at night. They go above and beyond the call of duty.

– Casey Potenzone
VP of Operations
Relegance
November 2004

GSA is provided with yearly briefings on AT&T and Networx DR capabilities. These briefings inform and educate the Government on the latest issues, trends, technologies, and our updated practices pertaining to disaster recovery. We will discuss the implications affecting the Networx program and inform the GSA of any actions AT&T plans to take to improve its readiness. The CPO works with the Government to reassess current disaster recovery plan/practices and planned improvements, to determine what changes to incorporate.

ATTACHMENTS

AT&T Disaster Recovery Example Deployments

A-1 Katrina Hurricane – August 29, 2005

Katrina made landfall near Buras-Triumph, Louisiana, just east of New Orleans, as a Category 4 hurricane on August 29th at 7:15 AM EDT. The Gulf Coast of Louisiana, Mississippi and Alabama sustained major devastation to the area in one of the worst natural disasters ever sustained in the United States. Anticipating the oncoming disaster, AT&T's Network Disaster Recovery (NDR) organization deployed most of its Operations Team, 4 Emergency Communications Vehicles (ECV), and a fly-away satellite unit to Louisiana and Mississippi. The NDR organization and Infrastructure Technical Services Group (ITSG) began deploying team members and equipment on Sunday, August 28th.

"We had small damage near New Orleans in the regional areas, but we were able to restore the service quickly within the first 24 hours, so we literally had no impact to our service in terms of long distance," said Hossein Eslambolchi, AT&T CTO & CIO. Throughout the hurricane and its aftermath the AT&T Network remained stable. Network restrictions were put in place to ensure the network remained stable and the Customer Service Organization established a Katrina Situation Room to handle all hurricane related restoration and provisioning requests. The Katrina Situation Room accounted for all customer requests for service in a single location to properly prioritize orders, route and escalate them correctly, and track the progress of the requests. While a very small number of facilities were still out of service, all major AT&T systems were returned to normal operations by noon EDT on August 31st.

Restoration efforts continued on a 24x7 basis and, as of August 31st all AT&T Central Offices were operational. In order to ensure the AT&T Network remained stable, Network restrictions were put in place in Texas, Oklahoma, Kansas, Arkansas, Missouri, Louisiana, Mississippi, Alabama, Florida, Georgia, and Tennessee, including the prohibition of any activity with the potential to disrupt 911 emergency service.

AT&T NDR deployment site at NASA's Stennis Space Center in Mississippi. The Stennis complex hosts several Federal government agencies. NDR is providing NASA with Internet connectivity and a phone bank. The phones are being used by shelter managers who are making calls out on behalf of the shelter residents in the area. September 1, 2005.

M0580v1

NDR ECVs provided humanitarian and administrative phone service at the National Guard Armory in Bogalusa, LA; at the Jefferson Parrish National Guard staging center in Weswego, LA, near the New Orleans airport; at a police facility set up in the Loyola Bus Station (New Orleans); and at Stennis International Airport, MS. The fly-away unit provided service for the team, for NASA's use and for the public at NASA's Stennis Space Center in Mississippi. ITSG provided emergency power, pumps and HVAC repairs for offices impacted by the storm. In addition, an ITSG generator provided back-up power for the L Troop State Police headquarters in Mandeville, LA. In addition, the AT&T Foundation matched AT&T employee donations for Hurricane Katrina relief efforts.

Overall, 53 Government Trouble Tickets / customer reports for outages attributed to Hurricane Katrina were created:

- 11 hours 8 minutes was the Mean Time to Restore (MTTR) for these reported outages.

- 19 of the reported troubles were resolved by AT&T's [redacted] within 2 minutes. These 19 troubles reflected circuits that were originally routed through the troubled area and [redacted] automatically re-routed them around the area.
- 9 facilities were re-routed manually to restoration facilities within 10 minutes.
- 13 LEC facilities were moved to restoration, or remapped to other facilities on the first day.

In addition to deployments in the affected area AT&T supported the Government by quickly deploying services in support of the relief efforts. An example is listed in **Table A-1.**

AGENCY	SITE/APPLICATION	CIRCUIT QUANTITY	REQUEST DATE	OPERATIONAL DATE
DHS/FEMA	North Hollywood Call Center	110 T1s (2640 Voice Trunks)	09/09/95	09/14/95
DHS/FEMA	Dallas Call Center	27 T1s (648 Voice Trunks)	09/09/95	09/13/95

Table A-1: Circuit Installation after Hurricane Katrina. *AT&T was able to install 137 T1.5 circuits shortly after the disaster struck.*

A-2 San Diego Wildfires – October 27, 2003

In the last week of October 2003, wildfires swept through northeastern San Diego County destroying over 2000 homes. On Sunday evening October 26, AT&T deployed a small group of NDR technology trailers and part of the NDR Team to San Diego as a precaution in case the fires damaged any network facilities.

The team and equipment were assembled at a staging location in Poway, California by mid-day on Monday, October 27. The team was positioned to provide a rapid recovery if any AT&T Network facilities were damaged or destroyed. Smoke and ash clouds continued to blanket the northern San Diego area on Monday and Tuesday.

The trailers remained in San Diego until Wednesday, October 29, 2003, after the risk from the fires had passed. The Emergency Communications Vehicle (ECV) that was deployed with the trailers remained in San Diego, along with a small team, to provide telephone service for a local assistance center.

A-3 Deployable Satellite Calling Center in Iraq – June 24, 2003

In early April 2003, AT&T Network Disaster Recovery designed and managed the assembly of six deployable satellite calling centers for use in Iraq. The calling centers were developed with AT&T Consumer Services (ACS) to provide telephone service to U.S. troops deployed in Iraq, supporting an ACS contract with the Army Air Force Exchange Service (AAFES), which manages U.S. military Post Exchanges (PXs) around the world.

Four NDR team members accompanied the equipment to Kuwait in early June 2003 to train AT&T contractors on the turn-up and maintenance of the calling centers. The first of the centers was brought online on June 24, 2003. In their first four months of service, the units provided over 900,000 calls from U.S. military posts in Iraq.

Each of the mobile sites is self-sufficient, with its own satellite dish, earth station equipment, power generator, air conditioning, and shelter.

A-4 World Trade Center Deployment – September 12, 2001

AT&T's Network Disaster Recovery (NDR) Team was activated immediately following the destruction of the World Trade Center towers on the morning of September 11, 2001. The collapse of the buildings, and the collateral damage that occurred, impacted AT&T's Local Network Services (LNS) capabilities.

NDR was deployed to support the recovery of those services and to provide emergency communications for the relief effort in lower Manhattan.

The first recovery trailers and team members arrived at a staging location in New Jersey by 6:00 a.m. EDT on Wednesday, September 12. A safe recovery location in northern New Jersey was secured early that afternoon. The team and its equipment were escorted to the site and the initial trailer setup was completed shortly after midnight.

On September 12, 2001, AT&T NDR deployed an Emergency Communication Vehicle (ECV) to provide emergency phone service for the New York City Police Department's command center near the World Trade Center disaster site. That ECV provided 44 voice lines for NYPD's use and dedicated 4 lines for use by the families of missing members of the NYPD and NYFD.

On Friday, September 21, the Manhattan ECV was moved to a location within the WTC disaster zone to provide emergency communications for New York City emergency response agencies and for humanitarian relief purposes (**Figure A-4**). The phone bank was set up in the Spirit of New York, a dinner cruise ship that was being used as a rehabilitation center for the WTC recovery crews. The ECV remained in service there until Thursday, October 4, 2001.

Figure A-4: An ECV deployed adjacent to the World Trade Center, September 2001. *ETVs play a critical role in early recovery efforts and beyond.*

Over 20,000 calls were placed over the ECV link at the NYPD deployment and over 36,000 calls were placed during the Spirit of New York deployment.

A second ECV was used at a recovery site in New Jersey to provide voice and data connectivity for the NDR team.

A-5 Tropical Storm Allison – Early 2001

M0340v1

Figure A-5: An NDR Emergency Communications Vehicle (left) and an NDR phone bank at a Red Cross shelter in Kirby, Texas (right). *The ECV was deployed following Tropical Storm Allison in early 2001.to provide humanitarian relief.*

In addition to supporting AT&T's network, the Network Disaster Recovery Team also used its Emergency Communication Vehicles (ECVs) to provide satellite-based deployable communication capabilities in support of humanitarian relief efforts. This was accomplished by provisioning satellite links through an ECV to the AT&T Network and establishing phone lines for outgoing calls (**Figure A-5**).

Cingular Disaster Recovery Example Deployments

Cingular's emergency preparedness program emphasizes prevention and recovery. Cingular has used this program to actively support events including Y2K, the NATO 50, the Pentagon 9/11 Disaster relief efforts, the DC mail anthrax investigations, and the 2002 Winter Olympics Crisis Management Unit's communications requirements. Some specific examples include the following:

B-1 Hurricane Katrina – August 29, 2005

- The Cingular network is built to withstand tropical storm-force winds, with cell sites backed up by high-capacity batteries or emergency generators. Cingular's Regional Network Operations Center (RNOC) also monitors and maintains the network around the clock, allowing Cingular to assess and handle any emergency situation within minutes.

- At the onset of Katrina, Cingular mobilized more than 100 teams of recovery technicians, consisting of over 800 personnel, to be ready to begin restoration efforts. These would come to include cell site surveys, placement and refueling of generators, placement of 30 COW and COLT (Portable cell sites), and replacement of other necessary equipment. More than 500 emergency generators were readied for dispatch with more than 800,000 gallons of fuel. Hundreds of additional network personnel and emergency equipment were put on stand-by in Florida and Georgia, ready to assist in recovery efforts.
- Cingular's network remained operational in Lafayette, Alexandria, Monroe (Louisiana); Tupelo (Mississippi); Huntsville, Montgomery, Dothan (Alabama); and Fort Walton, Pensacola (Florida). The network experienced minimal disruptions in Meridian, Columbus, and Starkville (Mississippi) and Birmingham (Alabama), while back-up generators minimized customer impact.
- Most of the network disruptions in Mississippi were in Jackson, Biloxi, Pascagoula, Bay St. Louis, Hattiesburg, Gulfport and Brookhaven. More extensive disruptions in Louisiana were primarily in Baton Rouge and New Orleans.
- Service fully restored in Mobile, AL, Jackson and Meridian, MS, and in Hammond and Houma, LA, substantially restored in Hattiesburg, Biloxi, and Gulfport, MS by 9/8/05.
- 50 percent of service in New Orleans, LA restored by 9/8/05.
- Many of the problems experienced with cell sites were due to the commercial power outages throughout the region. During the entire recovery effort, Cingular remained in close contact with all the wireline, power companies and public safety agencies.

B-2 2004 Hurricane Season

- During the **2004 hurricane season**, Cingular took the steps to prepare for storms and their aftermath, with the goal of maintaining service to customers or restoring it as quickly as possible throughout each event. Some preparedness measures included:
  - **Hurricane Ivan:** 560 portable generators, 8 COLTs/COWs staged, and 30 additional Network support personnel were provisioned to assist as needed.
  - **Hurricane Charley**: One hundred thirty portable generators were deployed at affected cell sites. Two COWs were deployed in the impacted areas to add coverage and capacity. Ten more COWs were on standby for additional calling capacity. Capacity at unaffected cell sites was boosted to handle the increase in call volume.

B-3 California Wildfires – 2003

- During the **California Wildfires in 2003**, less than 1 percent of Cingular's sites in San Diego and Los Angeles were impacted. Service restoration efforts brought nearly 80 percent of the overall impacted cell sites back online. Those that were not immediately restored were in areas inaccessible due to safety concerns, or were destroyed and have since been rebuilt. Cingular deployed 25 backup generators to augment commercial power losses at cell sites, and COWs were deployed to increase capacity.

B-4 Events of September 11, 2005

- During the September 11th events, Cingular worked closely with the National Communications System (NCS) and other Federal agencies to provide supplemental communications capacity and search capability in response to the disasters.

- **World Trade Center** - Working in conjunction with disaster relief teams and federal investigators Cingular helped perform Radio Frequency Triangulation on the Blackberry devices that many of the victims were wearing when the buildings collapsed. Cingular technicians sent constant messages to the devices looking for responses so that the search area could be narrowed.

The Cingular Interactive network remained operational during the entire crisis and often was the only means of communication when cell phones would not work. Cingular provided thousands of Blackberry devices to relief workers, at no cost, to help them communicate. Devices were also provided to doctors at area hospitals so patient vitals and condition could be sent in advance of hospital arrival. Cingular employees were on hand 24 hours a day for nearly a month.

- **Pentagon** - Cingular set up three mobile cell sites (COWS for “Cell on Wheels”) surrounding the Pentagon. Within hours of the plane crash, Cingular established semi-priority service for relief workers and during the following days programmed and distributed over 3000 cell phones. As relief workers entered the site, they were provided with IDs by the US Secret Service and cell phones for communication by Cingular. Cingular employees were on hand 24 hours a day charging phones and batteries and distributing them while maintaining a running phone list of the users. This provided quasi 411 service when relief workers needed to locate each other. In addition, family members of the victims were provided with handsets so rescue workers could keep them informed.

B-5 Oklahoma City Bombing – 1995

- Within 48 hours of the **Oklahoma City bombing in 1995**, Cingular tripled the number of voice channels in the downtown Oklahoma City area. This ensured open voice channels for everyone.

C-1 Global Crossing Disaster Recovery Examples

Global Crossing has proven its effective preparation, implementation and rapid response in critical emergencies. As the provider of the United Kingdom's Foreign Service Network, they were faced with a serious challenge when the facilities at the UK Consulate in New York were destroyed when the Twin Towers were attacked. Global Crossing moved quickly, implementing its continuity of operations plans and disaster recovery process for the UK. They were able to restore critical services within a matter of days and to provide full service restoration within 30 days of the attack. At the same time, many major organizations, including parts of the United Nations that were located on the southern end of Manhattan Island, did not achieve full service restoration for as much as six months.