

NRIC VII

---

September 23, 2004

FOCUS GROUP 1C

Analysis of Effectiveness of  
Best Practices Aimed at  
E911 and Public Safety

Report #1

---

## Table of Contents

1. Results in Brief
  - 1.1. Major Findings
  - 1.2. Report Timeline
2. Introduction
  - 2.1. Structure of NRIC VII
  - 2.2. Focus Group 1C Team Members
3. Background
4. Objective, Scope, and Methodology
  - 4.1. Objective
  - 4.2. Scope
  - 4.3. Methodology
5. Analysis and Findings
  - 5.1. Outage Analysis
    - 5.1.1. Compilation and Categorization of Outage Data
    - 5.1.2. Summary of Findings
    - 5.1.3. Analysis of Outage Data
  - 5.2. 911/E911 Best Practices
    - 5.2.1. Identification of those Best Practices most applicable to 911/E911 outages
  - 5.3. Architecture Vulnerabilities
    - 5.3.1. 911 Network Topology Reference Diagram
    - 5.3.2. Summary of Key Findings
    - 5.3.3. Network architecture areas most impacted by outages

6. Next Steps
7. Appendix 1 – Sources and Documentation
  - 7.1. Scrubbed 911/E911 Outage Data
  - 7.2. Network Topology Reference Diagram
  - 7.3. 47 C.F.R. § 63.100: Notification of Service Outage
  - 7.4. FCC 04-188: New Part 4 of the Commission’s Rules  
Concerning Disruptions to Communications
  - 7.5. NRSC Direct Cause and Root Cause Definitions
8. Appendix 2 – Definitions and Acronyms
  - 8.1. NENA Master Glossary of 9-1-1 Terminology

# 1 Results in Brief

## 1.1 Major Findings

### Outage Statistics

- The total number of outages reported pursuant to 47 C.F.R. § 63.100<sup>1</sup> from January 1, 2002 through March 31, 2004 that affected 911/E911 was 76
- The majority of 911/E911 outages affected less than 250,000 customers and lasted less than 5 hours. The exceptions were two outages that affected 1.76 million and 2.9 million customers respectively, and two other outages that lasted for 46 hours and 144 hours respectively

### Outage Causes

- The majority of 911/E911 outages were caused by cable damage and service provider procedural errors
- The primary causes of cable damage are inaccurate cable locates and failure to request a locate
- The primary causes of service provider procedural errors were insufficient training, insufficient supervision, inaccurate cable locates and unclear or unavailable procedures

### 911/E911 Best Practices

- 97 out of the 776 existing NRIC Best Practices from NRIC I-VI are applicable to 911/E911 outages and Public Safety

### 911/E911 Architecture Vulnerabilities

- Five areas of the 911/E911 architecture were identified as key vulnerabilities
  - Facility
  - CCS
  - Power Elements
  - Switches (local and tandem)
  - DCS

## 1.2 Report Timeline

Future 1C reports to the Council will include:

- Recommendations on ways to reduce E911 outages

---

<sup>1</sup> 47 C.F.R. § 63.100

[http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr\\_2003/oct\\_qtr/47cfr63.100.htm](http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr_2003/oct_qtr/47cfr63.100.htm)

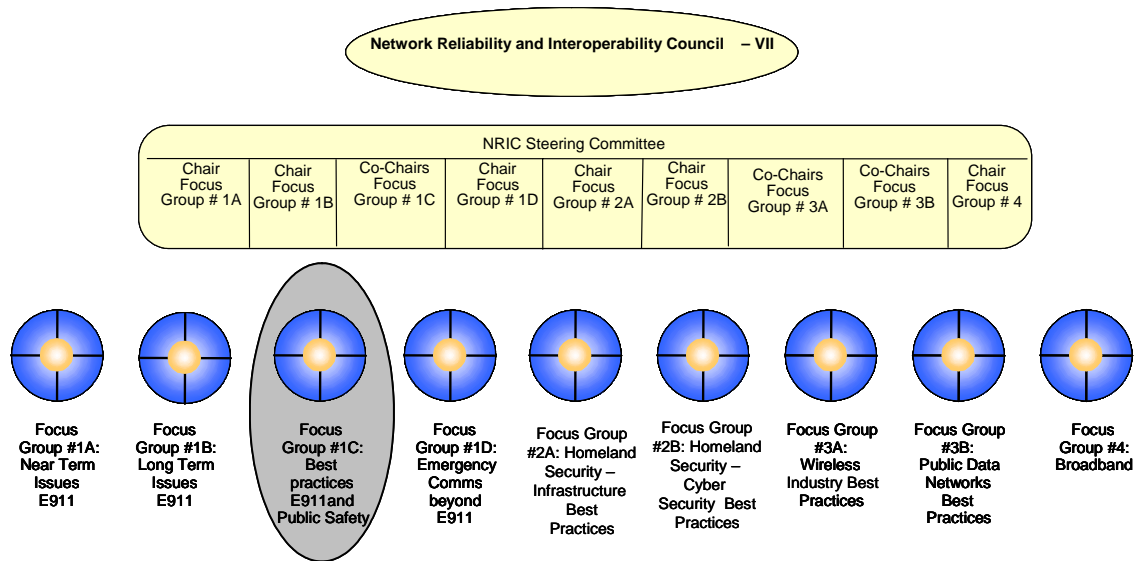
- Recommendations on ways to improve the relevance of the FCC-Reportable Outage data for improving Emergency Communications, including defining direct causes and root causes which are better attuned to E911
- Refining the language that is contained in the E911 NRC/NRIC Best Practices to make it more precise so that E911 outages will be prevented and the level of compliance with each Best Practice can be reliably measured
- An analysis of the effectiveness of the Best Practices that have been developed to address E911 and Public Safety

## 2 Introduction

This report documents the efforts undertaken by the Network Reliability and Interoperability Council (NRIC) VII Focus Group 1C with respect to the 911/E911 outage analysis, identification of applicable Best Practices, and identification of architecture vulnerabilities.

### 2.1 Structure of NRIC VII

The structure of the Network Reliability and Interoperability Council is as follows:



## 2.2 Focus Group 1C Team Members

Today, Focus Group 1C consists of 25 members, though we expect there will be some additions and deletions in the future.

The group was broken into four subgroups to address the different portions of this report. The subgroups each focused on one of the following: Outage Analysis, Best Practice Identification, 911 Network Topology Reference Diagram development, and Vulnerabilities Analysis.

### Focus Group 1C Members

Name	Company
Bonnie Amann	Sprint
Jay Bennett	Telcordia Technologies
Robert Burkhardt	Nextel
Rick Canaday	AT&T
Doug Edmonds	Northwest Central Dispatch
Darryl Foster	Cox Communication
Ann Gasperich	Houghton County 9-1-1
Bob Iwaszko	Verizon Wireless
Percy Kimbrough	SBC
Bill Klein	ATIS
Richard Krock	Lucent Technologies
Gail Lassiter	BellSouth
Marc Linsner	Cisco Systems, Inc.
Spilios Makris	Telcordia Technologies
Ron Mathis	Intrado
Bob Oenning	Washington State E911
Janice Partyka	TechnoCom Corp.
Nancy Pollock	Metropolitan 911 Board
Karl Rauscher	Lucent Technologies
Jim Runyon	Lucent Technologies
Robert Schafer	MCI
Thom Selleck	AT&T
Kevin Smith	Nortel Networks
Whitey Thayer	FCC
Rachel Torrence	Qwest

### 3 Background

The Network Reliability and Interoperability Council was originally established to study the causes of service outages and to develop recommendations to reduce their number and their effects on consumers.<sup>2</sup> NRIC's I-IV concentrated on reliability concerns in a number of areas including signaling (SS7), fiber cuts, switching systems, power failures, fires, 911 outages, and digital cross-connect systems. Reports and trends in these areas were studied and recommendations on what level of service outages ought to be reported to the FCC were made. A limited number of Best Practices to address these areas of concern were also developed.

NRIC V implemented a "voluntary one-year trial with participation by Internet Service Providers, CMRS, satellite, cable, and data networking service providers to alert National Communications System/National Coordinating Center for Telecommunications (NCS/NCC) of outages that are likely to have significant public impact."<sup>3</sup> This was the first step NRIC took in expanding its review of outages beyond wireline service providers.

NRIC VI expanded its focus to include key types of public communications networks, including wireless, Internet, satellite, cable, and paging. The NRIC VI Focus Group 1 was specifically chartered to focus on homeland security and public safety. Of utmost importance, especially in light of the events of September 11, 2001, was the development of recommendations to ensure the security and sustainability of public communications networks. The result was the development of a large number of Best Practices.

Closely tied to these objectives was the work of Focus Group 2, which focused on network reliability. This group conducted a Voluntary Outage Reporting Trial for communications networks not required to report outages on a mandatory basis under the regulations in place at that time. The Focus Group also reviewed the mandatory outage reporting requirements with respect to potential changes, and reported on the analysis performed on this outage data by the NRSC.<sup>4</sup>

NRIC VII combines the earlier focus of Public Safety and outage reporting, as focus group 1C focuses on the reportable outages that affect 911/E911 services,

---

<sup>2</sup> [www.nric.org](http://www.nric.org)

<sup>3</sup> Ibid.

<sup>4</sup> NRIC VI Focus Group 2 - Network Reliability, Final Report, November 17, 2003  
[http://www.nric.org/fg/charter\\_vi/fg2/FG\\_2\\_Final\\_Report\\_ver\\_120103.doc](http://www.nric.org/fg/charter_vi/fg2/FG_2_Final_Report_ver_120103.doc)

the Best Practices applicable to E911 and the vulnerabilities in the E911 network. We expect that future NRICs may continue the analysis of outages, expanding that focus to include wireless and data network outages, which are now reportable under FCC 04-188<sup>5</sup>.

## 4 Objective, Scope, and Methodology

### 4.1 Objective

The NRIC VII Council has been charged with reporting on ways to improve emergency communications networks. Per the NRIC VII Charter, Focus Group 1C is responsible for performing an analysis of the effectiveness of Best Practices aimed at E911 and Public Safety over the course of NRIC VII.

Report #1 addresses the first interim deliverable identified in the NRIC VII Charter for Focus Group 1C:

“The Council shall present a report containing its analysis of 63.100 outages related to 911/E911 and the Best Practices that are most applicable to E911 outages. The report shall also identify E911 architecture vulnerabilities.”<sup>6</sup>

### 4.2 Scope

This report contains the following:

- Analysis of outages related to 911/E911 that have been reported pursuant to 47 C.F.R. § 63.100<sup>7</sup>
- Identification of which Best Practices are applicable to E911 outages
- Identification of E911 architecture vulnerabilities

The scope of this document is limited to outages related to 911/E911 that have been reported pursuant to 47 C.F.R. § 63.100. The team did not review data from outages that were not reportable or that did not affect 911/E911 services.

The scope of future deliverables for Focus Group 1C will include the analysis of the effectiveness of Best Practices applicable to E911 outages, as well as recommendations for reducing E911 outages. This report is limited to the identification of the applicable Best Practices and architecture vulnerabilities.

---

<sup>5</sup> New Part 4 of the Commission’s Rules Concerning Disruptions to Communications, FCC 04-188 [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-04-188A1.doc](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-188A1.doc)

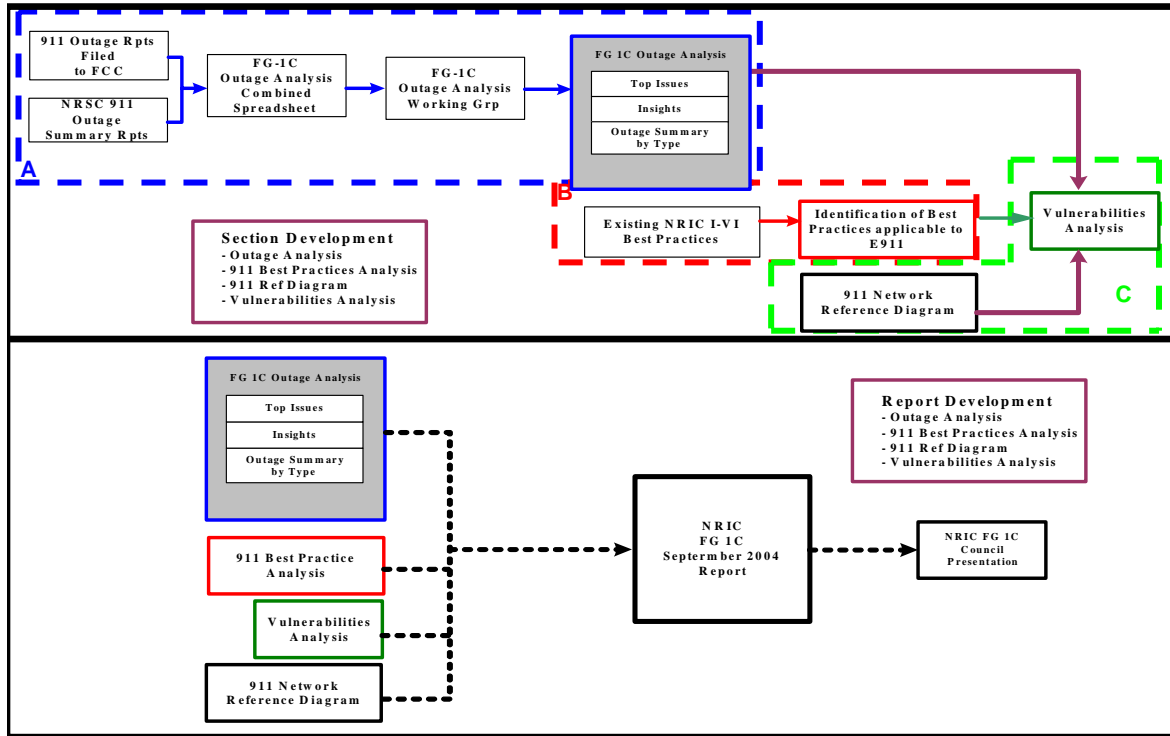
<sup>6</sup> NRIC VII Charter, [www.nric.org](http://www.nric.org)

<sup>7</sup> 47 C.F.R. § 63.100 [http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr\\_2003/oct\\_qtr/47cfr63.100.htm](http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr_2003/oct_qtr/47cfr63.100.htm)

### 4.3 Methodology

Below is an illustration of the methodology that was followed by Focus Group 1C in completing this report.

Exhibit 4.3 – Report Methodology



#### A. Outage Analysis Methodology

1. The team identified the timeframe of the data it would use for the outage analysis. Prior to NRIC VI, the focus of Best Practices was on the traditional wireline networks. NRIC VI changed the landscape by developing and incorporating Best Practices addressing wireless networks. Consequently, when determining what time frame would be used in the outage analysis, Focus Group 1C chose to analyze outage data for 2002, 2003, and the first quarter of 2004 as this was the time frame during which a significant number of Best Practices were developed. It was also felt that Best Practices that impact 911 have evolved significantly due to the efforts of previous NRIC's, making earlier outage data less relevant to current Best Practices.
2. Outage data was then compiled by obtaining two sets of data:
  - The FCC data on outages related to 911/E911 that have been reported pursuant to 47 C.F.R. § 63.100 from January 2002 through March of 2004. The initial number of outage incidents received from the FCC for

this purpose was 84. These incidents contained raw data as reported to the FCC by the carriers.

- 80 NRSC summary data outage incidents based on E911 outages that were reported pursuant to 47 C.F.R. § 63.100 from January 2002 through March of 2004. These reports summarized the same FCC data and categorized each outage within three primary categories (Failure, Direct Cause, Root Cause). In all cases, these reports summarized outages that were reported to the FCC. These reports were reconciled with the FCC data to ensure consistency.
3. The Outage Analysis subgroup members reviewed the individual outage reports from the two sources, and confirmed that the outage did in fact affect 911 services. If this was not the case, the outage was not included in the analysis. It was noted that virtually any telephone service outage can impact the capability to dial 911, but only those outages where carriers had indicated a 911 impact were analyzed. Also not included were any reports that were initially filed pursuant to 47 C.F.R. § 63.100, but then were later withdrawn by the filing company because it was later determined that the outage did not meet the criteria requiring it to be reported. Through this review and reconciliation process, the subgroup determined that 76 of the outage incidents provided to the team by the FCC and NRSC affected 911/E911 services and should be included in the analysis.
  4. Once the team identified the outages to be included in the analysis, the individual outage reports from both sources were reviewed and pertinent information was captured in a combined spreadsheet. Information captured from the reports included:
    - Date of outage
    - Duration of outage
    - Potential customers affected
    - NRSC Failure Category
    - NRSC Direct Cause Category
    - NRSC Direct Cause Sub-Category
    - NRSC Root Cause Category
    - NRSC Root Cause Sub-Category
  5. It was decided by the team that for consistency with other reporting groups, the NRSC definitions would be used in identifying the root cause, direct cause, failure category, and all related sub-categories. These definitions can be found in Appendix I.
  6. Outage information was requested from states where the 911 program tracks outages. This data was not included in the analysis due to inconsistencies with the NRSC categories, but appeared to confirm the analysis of the 47 C.F.R. § 63.100 reports

7. The compiled outage data was then analyzed by the Outage Analysis subgroup to identify trends, key findings, and areas of concern. Graphs are depicted in the Outage Analysis section in this report.

### ***B. Best Practice Identification Methodology***

1. The full list of existing NRIC Best Practices totaling 776 were obtained from the NRIC website.<sup>8</sup>
2. The Best Practices were sorted in order to identify 911/E911 practices using key word searches for words such as Public Safety, 911, and Emergency Services.
3. A total of 97 of the existing NRIC Best Practices were identified by the Best Practices subgroup as being applicable to 911/E911.

### ***C. Architecture Vulnerability Identification Methodology***

1. A 911 Network Topology Reference Diagram was developed to “level-set” the team when assessing the architecture vulnerabilities. This reference diagram is a high level graphic illustration of network components and architectures that facilitated the analysis by allowing the team to compare “apples to apples” when dealing with differing technologies and functionalities. This reference diagram can be found in the Findings and Analysis Section, as well as in Appendix I.
2. The Architecture Vulnerability subgroup referred to each of the 76 outages contained in the analysis, and using the reference diagram as a map, identified in which area of the network each outage occurred.
3. This data was aggregated and analyzed for trends identifying the most vulnerable areas of the 911/E911 network.
4. As per NRIC VI, vulnerability is defined as a characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.<sup>9</sup>

---

<sup>8</sup> <http://www.bell-labs.com/cgi-user/krauscher/bestp.pl>

<sup>9</sup> Network Reliability and Interoperability Council VI, Homeland Security - Physical Security (Focus Group 1A) Final Report, Issue 3, December 2003

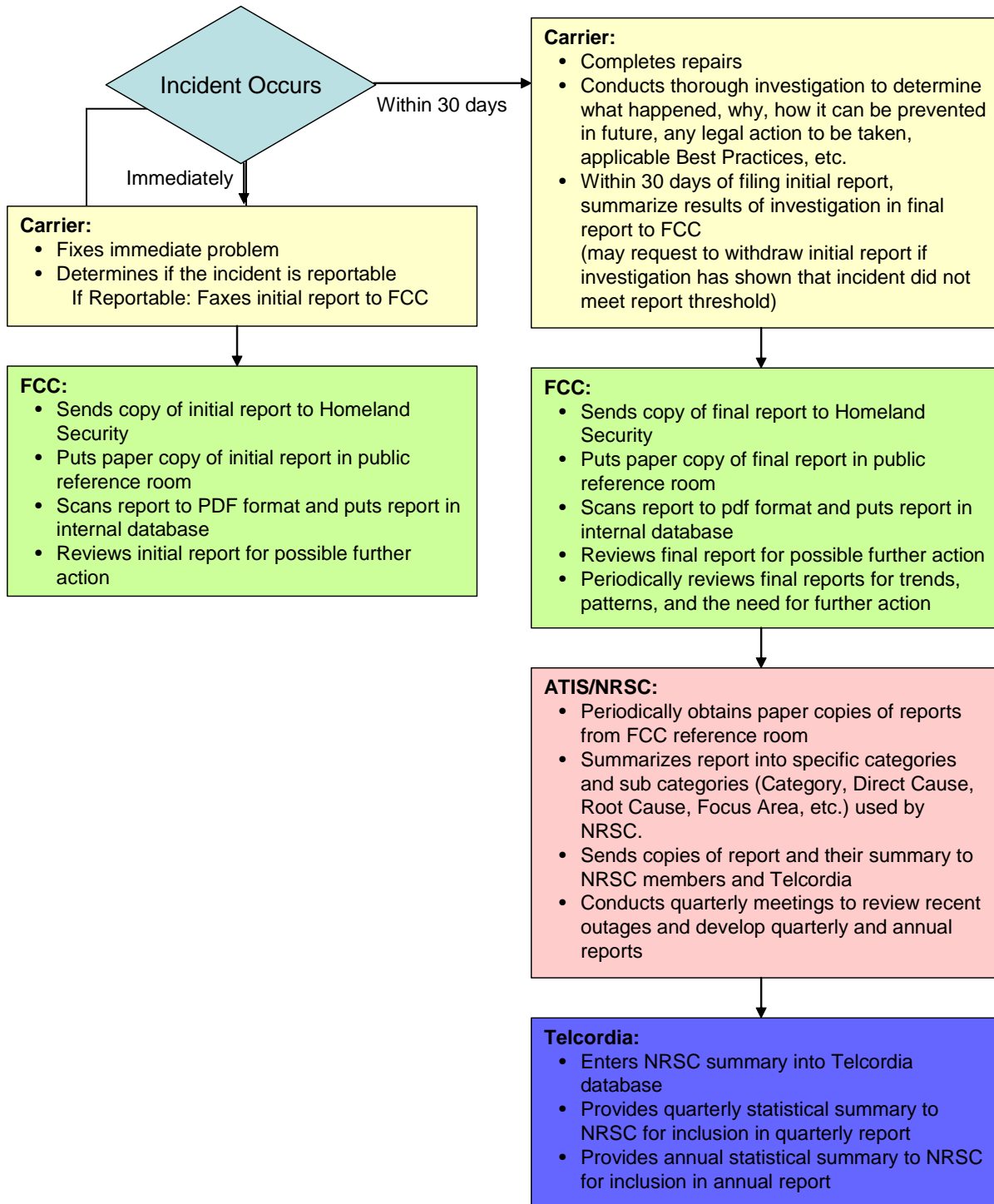
## 5 Analysis and Findings

### 5.1 *Outage Analysis*

#### 5.1.1 **Compilation and Categorization of Outage Data**

As was mentioned in the methodology section, the outage analysis was performed based on data received from two sources: the FCC and the NRSC. It is useful to understand how these two entities generate the data that was provided to the focus group for analysis. The diagram below shows the flow of information from the time an outage takes place to the time it is captured as data in the FCC and NRSC databases. The chart is color coded by the entity taking the action listed in each box (e.g., FCC, carrier, etc.)

**Exhibit 5.1.1 A - Outage Reporting Process**



In addition, the team agreed to use the established NRSC definitions in identifying the direct cause, root cause, and failure category of each outage.

The direct cause is defined as the event, action, or procedure that triggered the incident. While a carrier may identify the direct cause of an incident in any way that it deems appropriate, for its analysis of outages the Network Reliability Steering Committee (NRSC) has defined and utilizes the direct causes listed in the "Direct Cause Definitions", found in Appendix I of this document. It is recommended by the NRSC that for uniformity in reporting these definitions be implemented when determining the direct cause of an outage.<sup>10</sup>

The root cause is defined as the key problem, which once identified and corrected prevents the same or a similar problem from recurring. Typically the root cause can be determined through a thorough reading of the "Background of the Incident". However, it is often necessary to read both the "Background of the Incident" and "Steps Taken to Prevent Recurrence of the Incident" to determine the true root cause. In today's technology, two or more problems may be closely linked and require detailed investigation. However, in any single incident there should be only one root cause. While a carrier may identify the root cause of an incident in any way that it deems appropriate, for its analysis of outages the Network Reliability Steering Committee (NRSC) has defined and utilizes the root cause listed in the "Root Cause Definitions", found in Appendix I of this document. It is recommended by the NRSC that for uniformity in reporting these definitions be implemented when determining the root cause of an outage.<sup>11</sup>

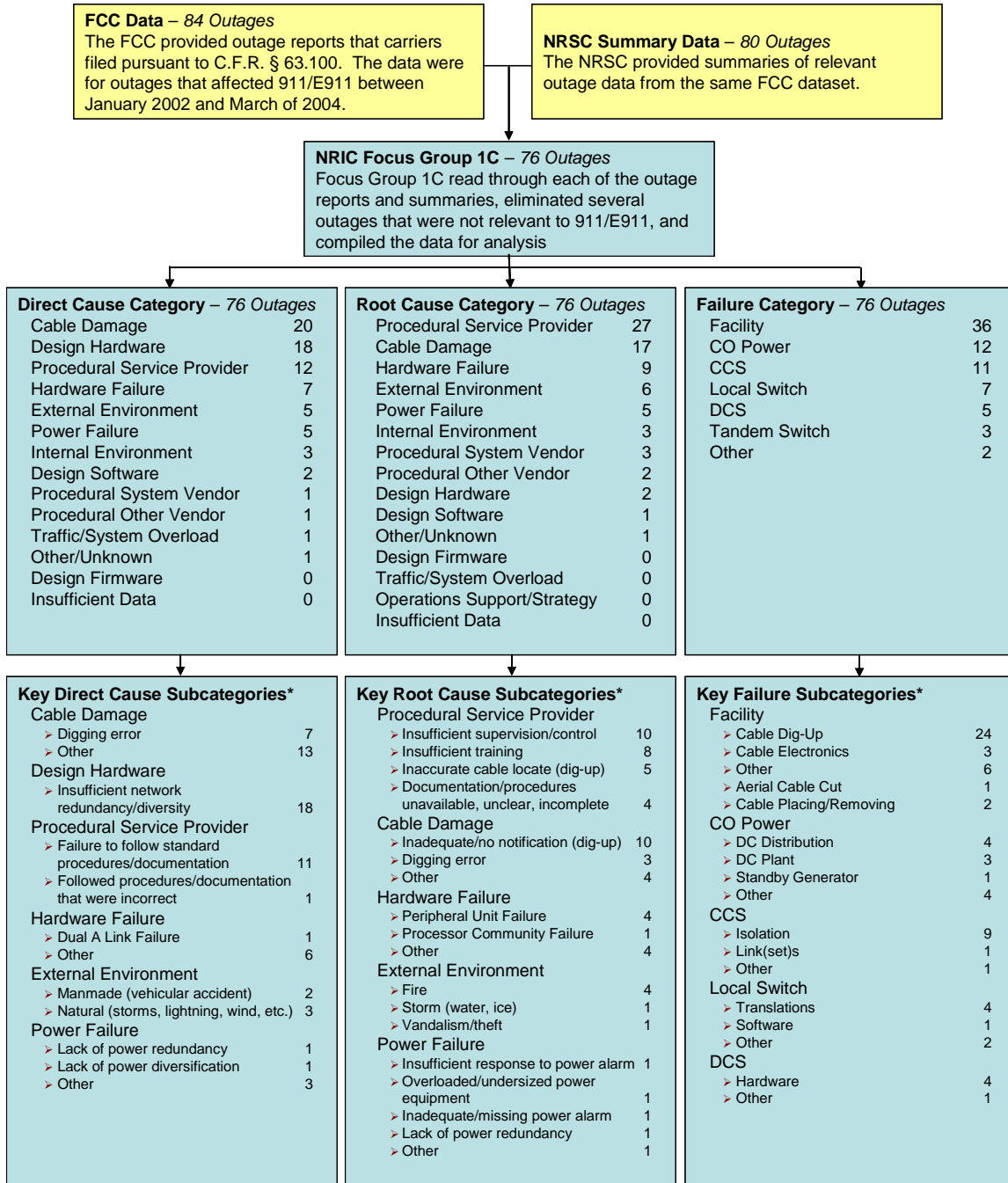
In many cases there were NRSC subcategories that were applied to an outage as well. The following diagram shows the hierarchy of this methodology, and highlights some of the key subcategories applied to a large number of outages.

---

<sup>10</sup> Network Reliability Steering Committee; <http://www.atis.org/nrsc/index.asp>

<sup>11</sup> Ibid.

### Exhibit 5.1.1 B - Hierarchy of outage characterizations



\* Only subcategories with five or more outages are expanded in this table, and therefore the subcategory sums do not equal 76.

### 5.1.2 Summary of Findings

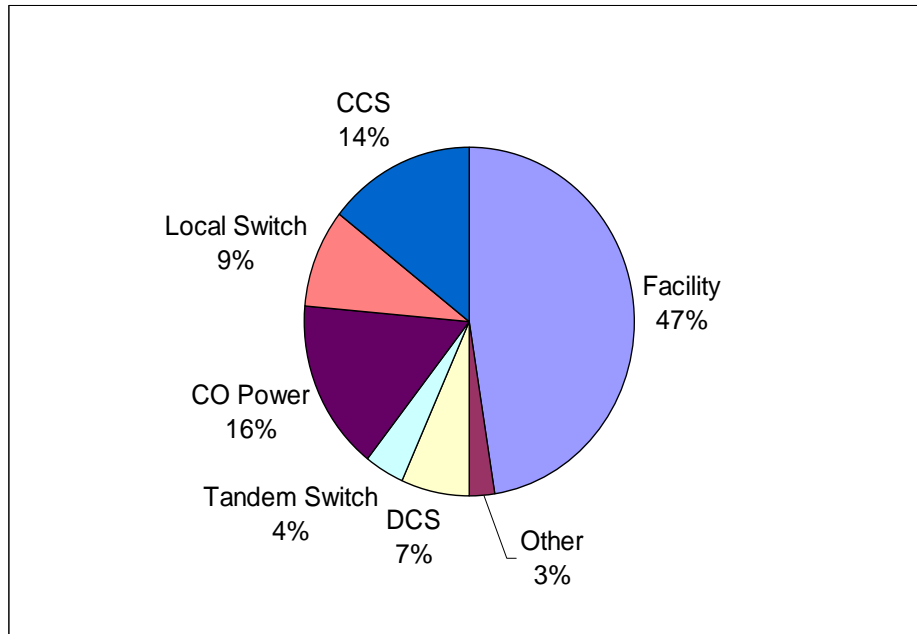
- The total number of outages reported pursuant to 47 C.F.R. § 63.100 from January 1, 2002 through March 31, 2004 that affected 911/E911 was 76

- The majority of 911/E911 outages (47%) took place within the network facility or plant. Most of those (66%) were due to cable dig ups
- The majority (57%) of 911/E911 outages are caused by either cable damage or service provider procedural errors
  - 27 outages (35%) listed a service provider’s procedural error as the root cause
  - 17 outages (22%) listed cable damage as the root cause
- In further breaking down these results, the primary causes of service provider procedural errors were:
  - lack of training (29%)
  - lack of supervision (29%)
  - inaccurate cable locate (17%)
  - incomplete procedures (14%)
- In further examination of the cable damage results, the primary cause is the failure to request a locate and other digging errors (76%)

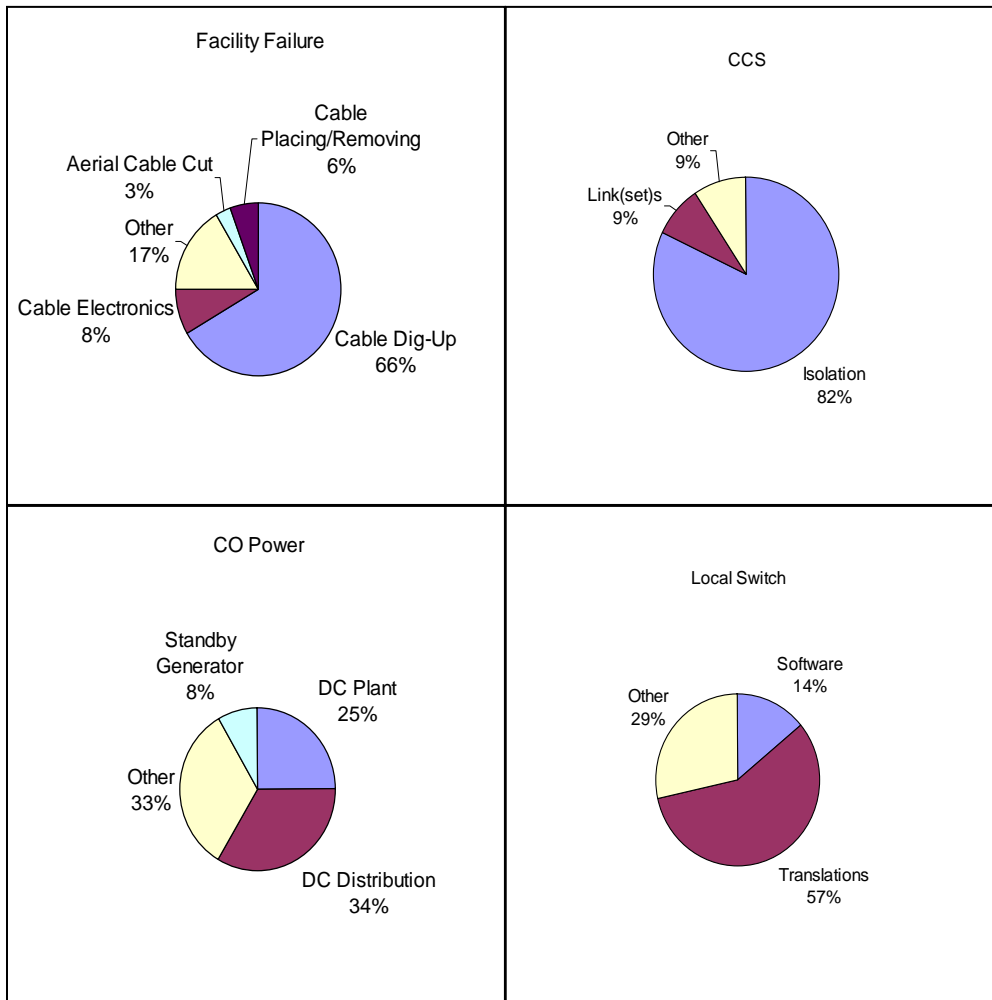
### 5.1.3 Analysis of Outage Data

The outage data was analyzed starting with Failure Category, Direct Cause and Root Cause. Further analysis was done by sub-category to identify the key causes of outages. The link to a lack of diversity was also examined to determine how many outages were potentially affected by a lack of network or equipment diversity on the part of either the carrier or PSAP. Finally, the length of time and number of people affected by outages was examined and chartered. Below is a graphical representation of the analysis.

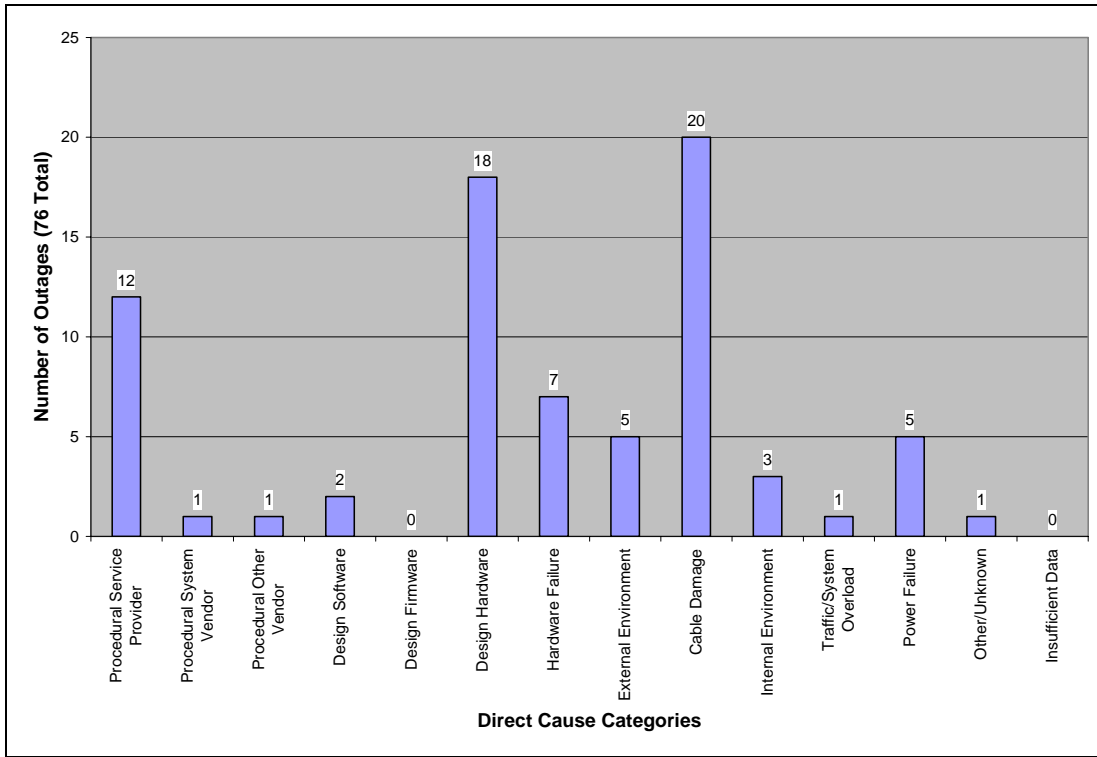
**Graph 5A-1: Percentage of outages by failure category**



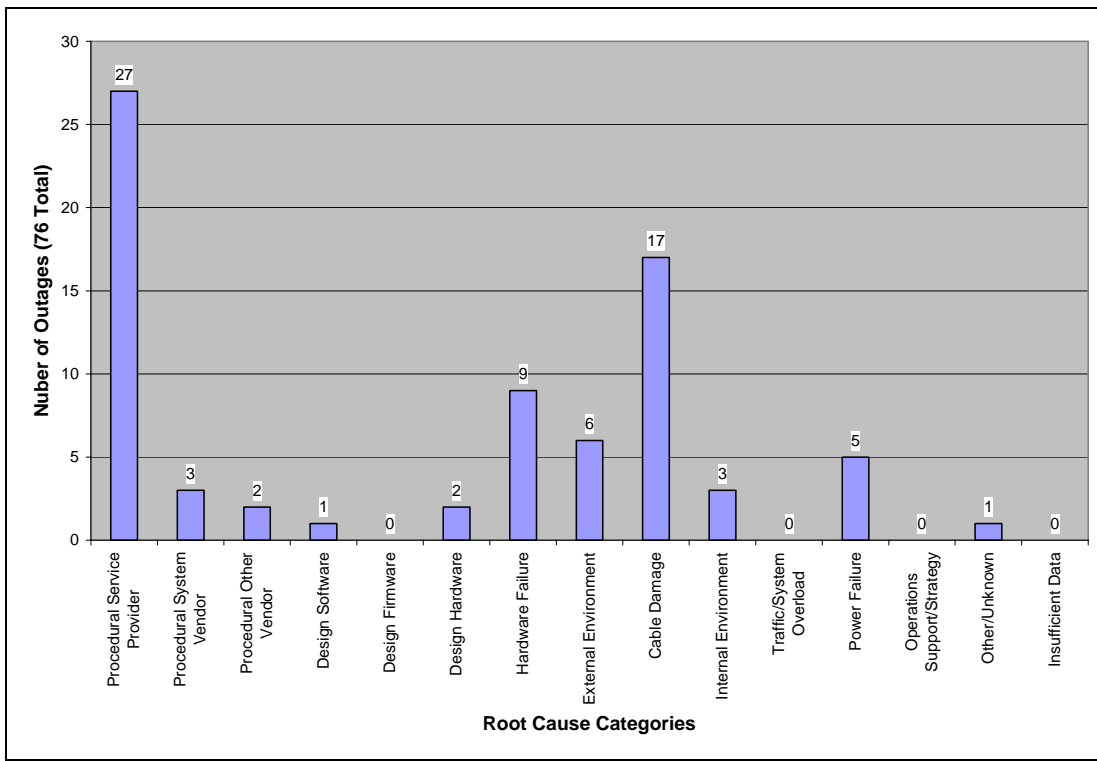
**Graph 5A-2: Percentage of outages by failure subcategory**



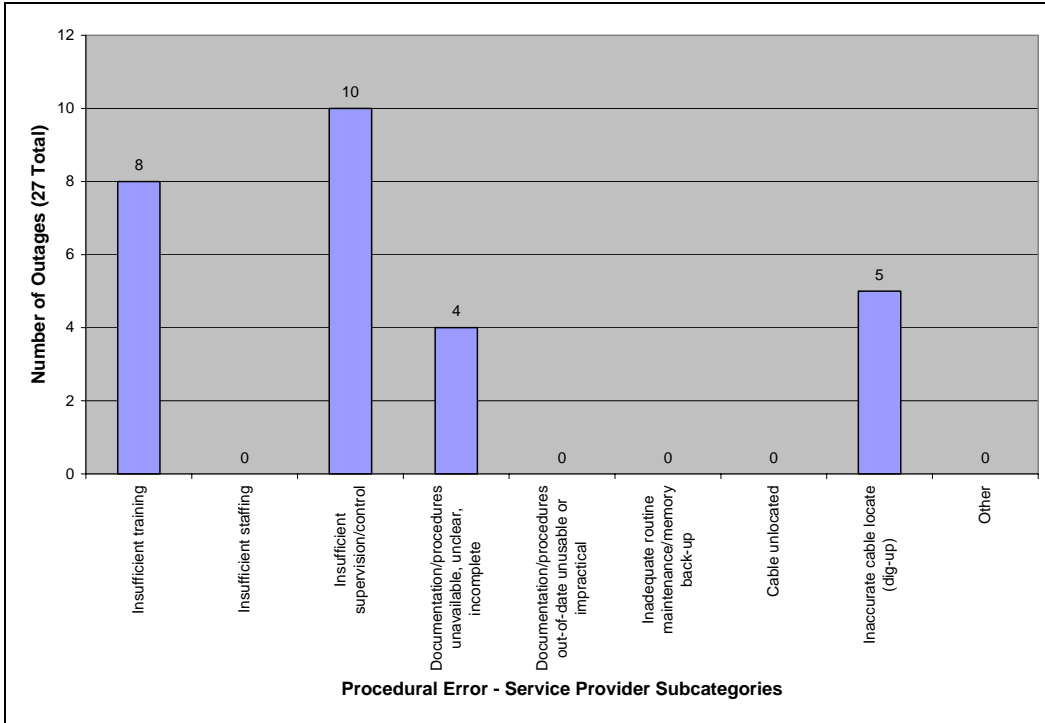
**Graph 5B: Number of outages by direct cause category**



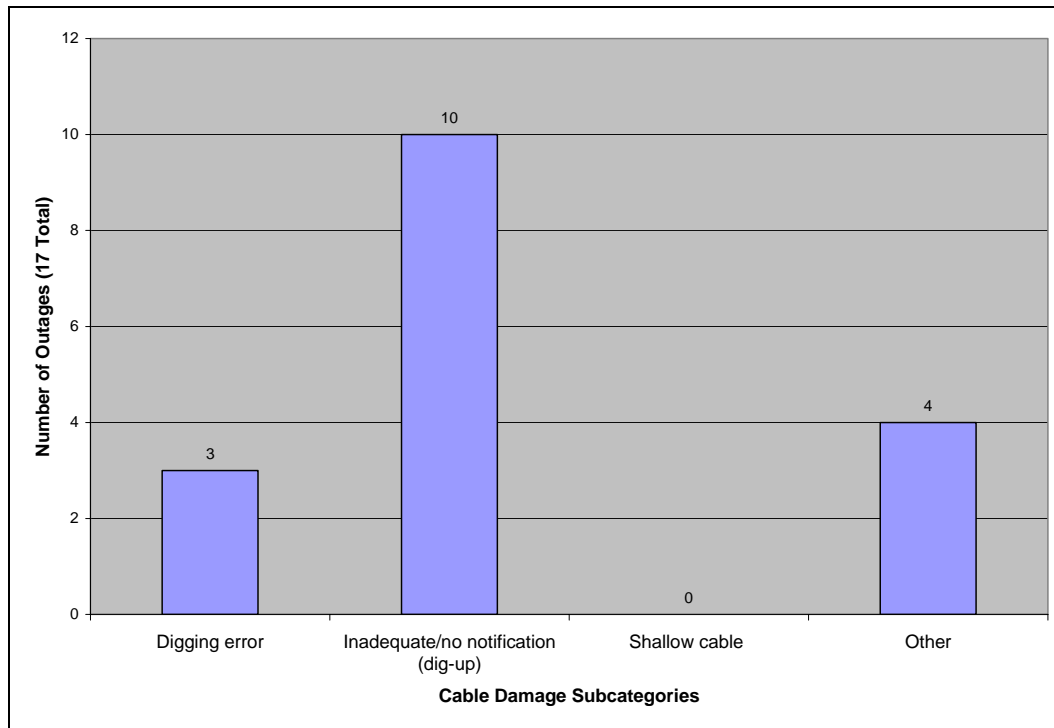
**Graph 5C-1: Number of outages by root cause category**



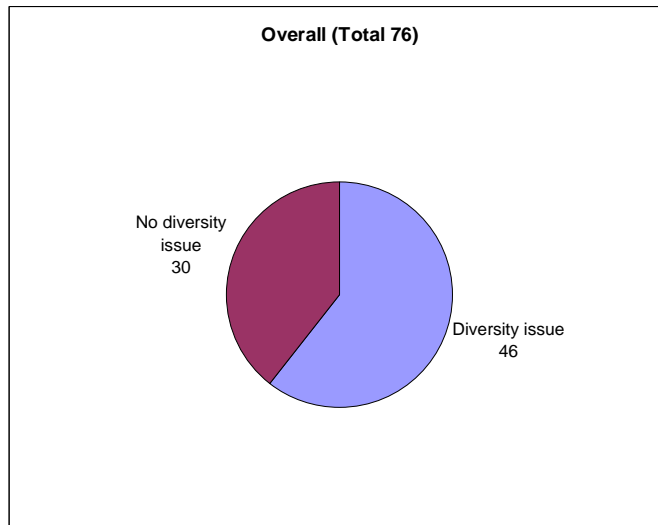
**Graph 5C-2: Number of outages by service provider procedural error root cause subcategories**



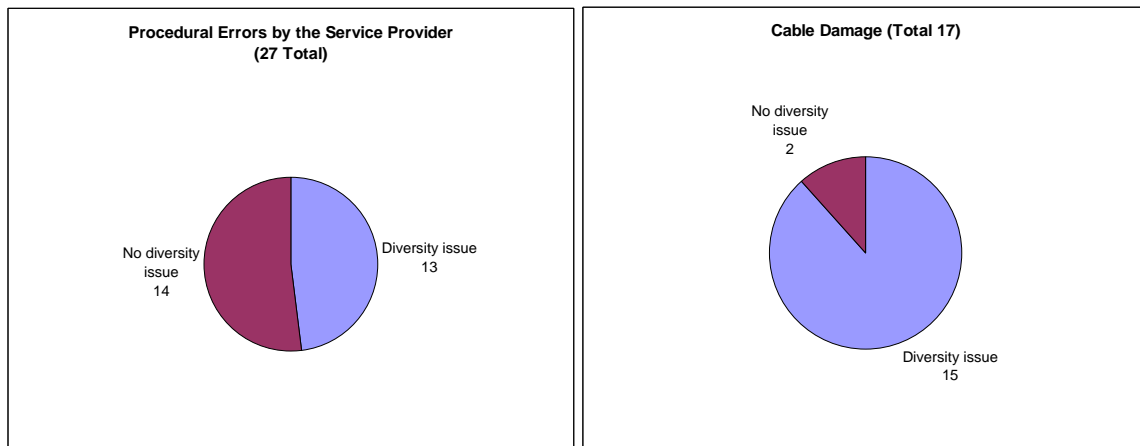
**Graph 5C-3: Number of outages by cable damage root cause subcategories**



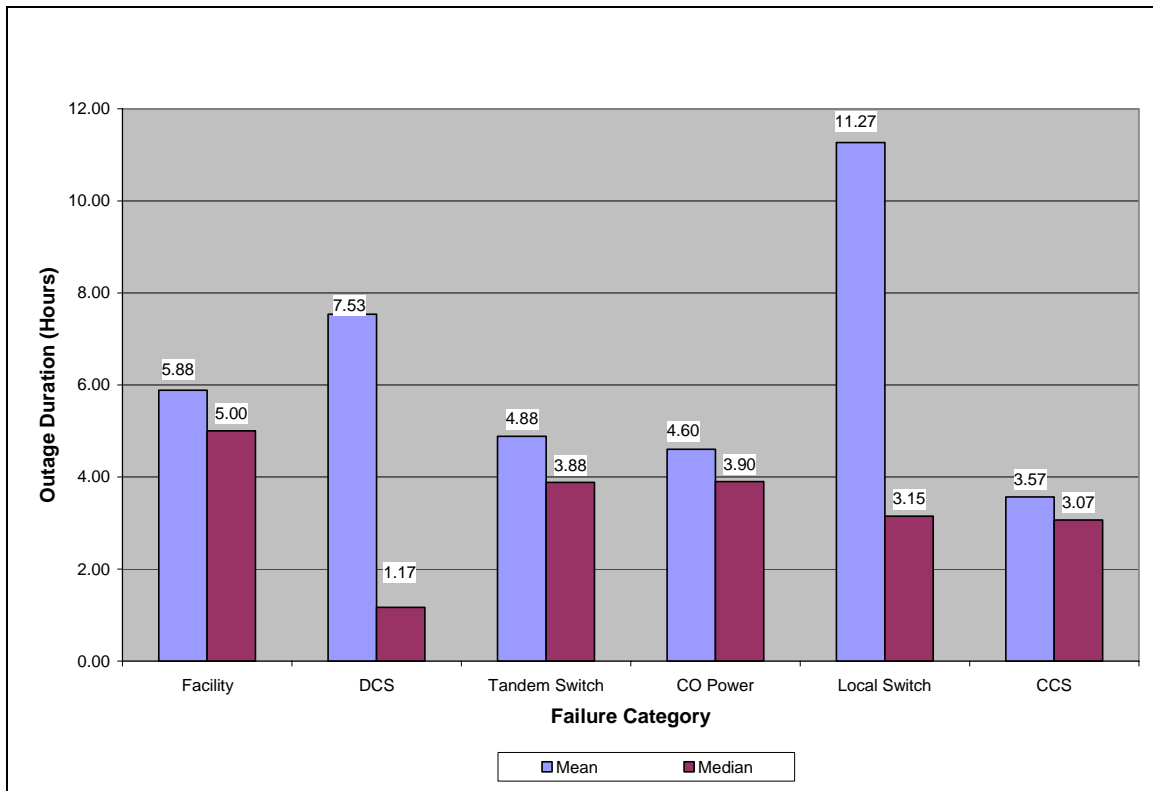
**Graph 5D-1: Number of outages that can be linked to lack of diversity**



**Graph 5D-2: Number of outages that can be linked to lack of diversity by root cause**



**Graph 5E: Duration of outage by failure category\***



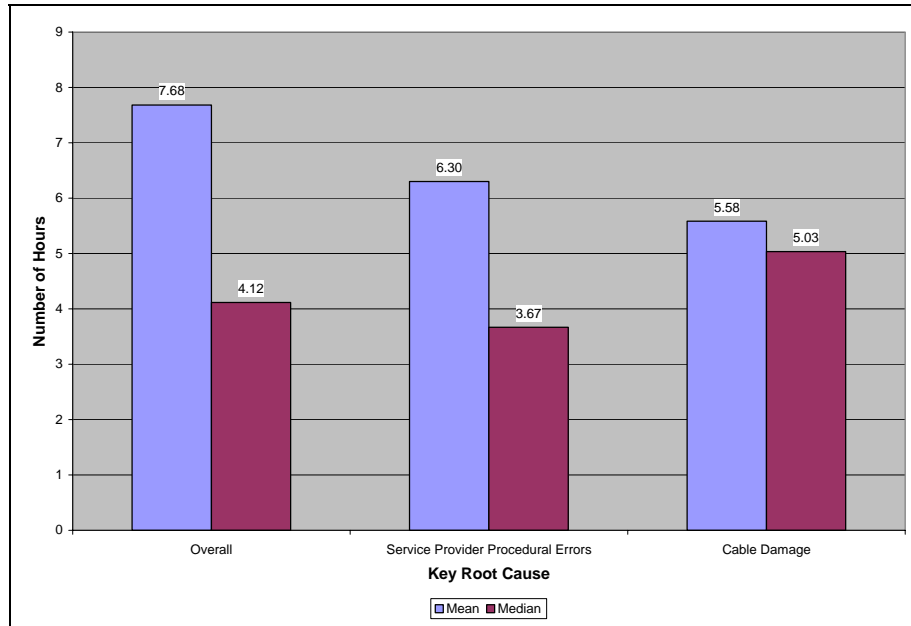
\* The “Other” category was removed from this chart. Of the two outages in this category, one of the data points was an outlier (144 hour outage due to severe winter weather).

The disparity between the mean and the median outage durations is notable for DCS and Local Switch categories. Closer investigation of the data shows that outlier data points are responsible for these sharp differences.

Of the five outages categorized as DCS failures, there is a significant gap between the duration of the two longest outages and the other three. The relatively small number of outages compounded by the large gap in the time periods results in a pronounced positive skew to this data.

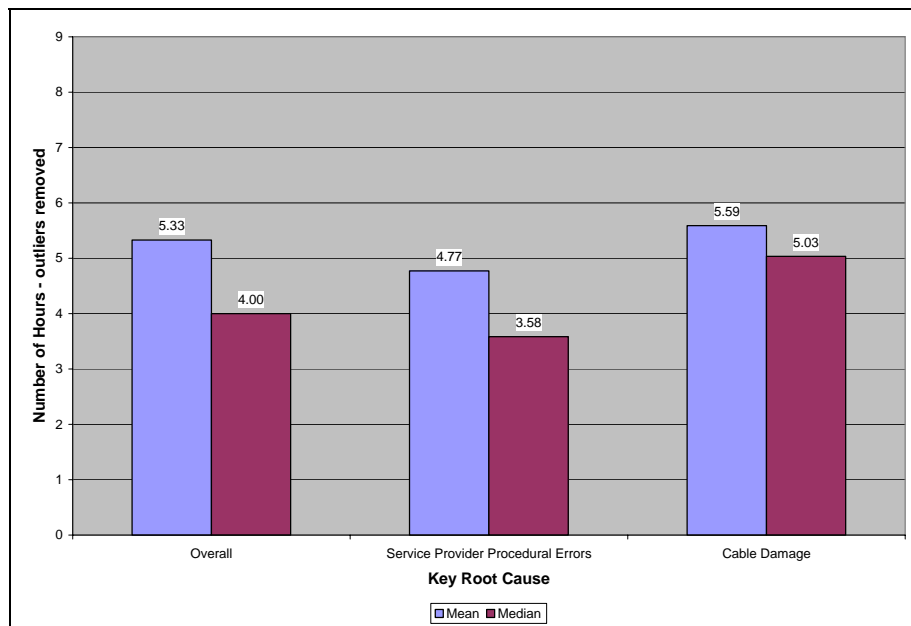
The Local Switch data are skewed by outage 04-013 which is an outlier in duration (46 hours). Removing this outage, which was caused by an improper change to the data on the local switch and did not trigger the notification system, would greatly reduce the gap between the mean and the median for the Local Switch category.

**Graph 5F-1: Duration of outage by key root cause categories (all data)**

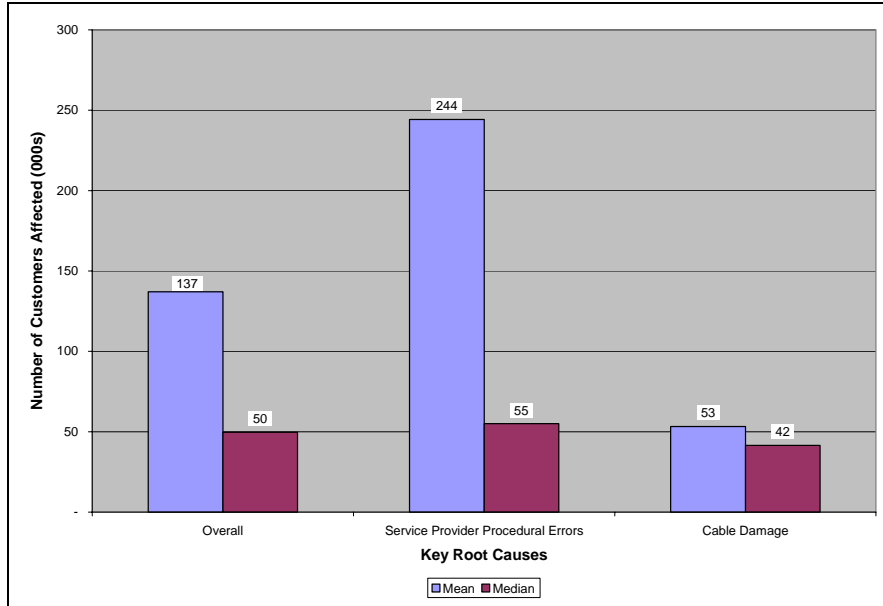


Two specific outlier data points skew the data considerably resulting in higher than expected disparity between the mean and the median of both the “Overall” numbers and the “Service Provider Procedural Errors”. Removing outage number 04-013 (46 hours) and outage number 02-135 (144 hours) brings each of these categories closer to expected results, though the Overall data still indicate a skew towards longer outages (see Graph 5F-2).

**Graph 5F-2: Duration of outage by key root cause categories (outliers removed)**

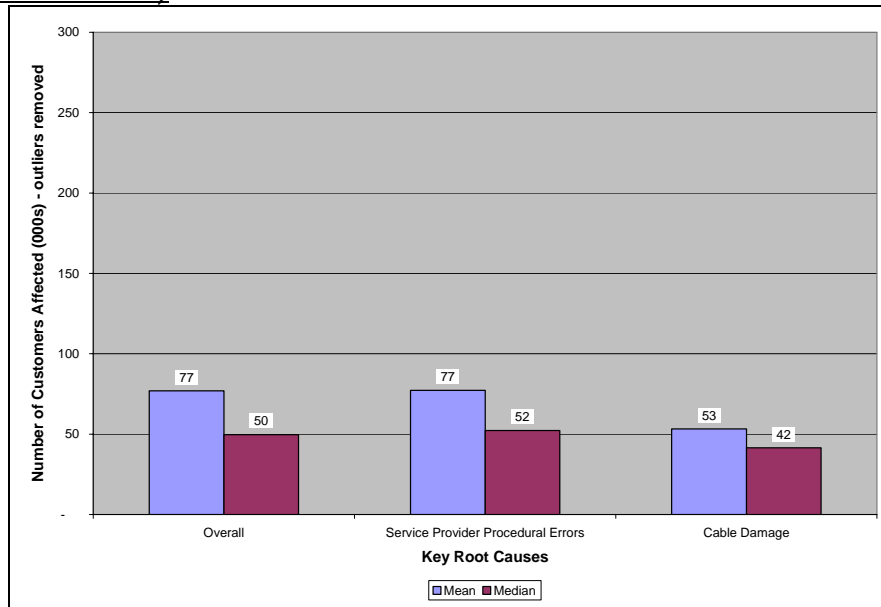


**Graph 5G-1: Number of affected customers by key root cause category (all data)**

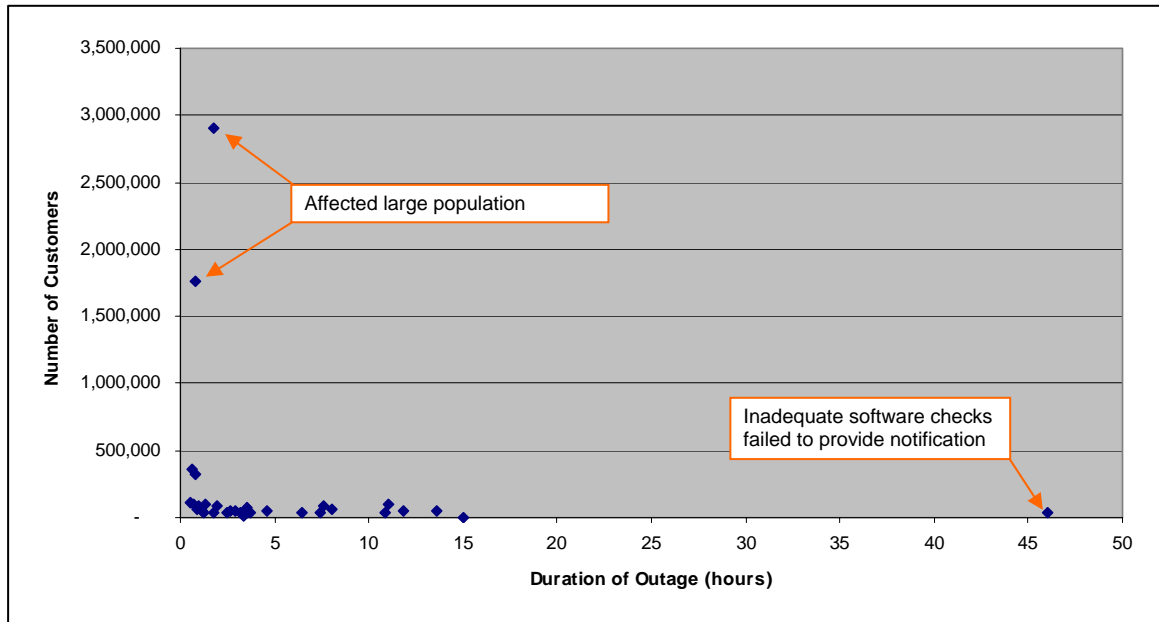


Two specific outlier data points skew the data for “Overall” and “Service Provider Procedural Errors”. Included in the data analysis for both of these categories are two outages that affected 2.9 million and 1.76 million customers. Removal of these two outlier data points provides a more realistic view of the mean, which still indicates a positive skew (see Graph 5G-2).

**Graph 5G-2: Number of affected customers by key root cause category (outliers removed)**



**Graph 5H: Depiction of outage duration (hours) and number of customers affected**



## 5.2 911/E911 Best Practices

### 5.2.1 Identification of those Best Practices most applicable to 911/E911 outages

Through a series of key word searches, the Best Practices subgroup identified a total of 97 Best Practices that are applicable to 911/E911 outages as well as related to Public Safety. The Best Practices identified can be grouped into the following categories: Diversity/Redundancy; Contingency/Emergency Planning; Data Assurance/Traffic Management; Media/Public Awareness; Emergency Management; Prevention; Cooperation/Communications with Emergency Service Entities.

#### Exhibit 5.2.1 - Best Practices most applicable to E911 outages

Best Practice Number	Best Practice Text
Diversity/Redundancy	
6-6-0580	<p>Critical Response Link Redundancy/Diversity and Security - The redundancy and diversity concepts set forth in Best Practice 6-5-0566 should be applied to other network links considered vital to a community's ability to respond to emergencies. Security practices and concepts set forth in the Security Best Practices should be applied to the critical systems supporting Link Redundancy and Diversity. Critical links include point-to-point private circuits used by Public Safety networks for radio site communications, but obtained from commercial landline communication providers. Types of links that are critical to the provision of emergency aid include communication links from the PSAP location to:</p> <ul style="list-style-type: none"> <li>Law enforcement dispatchers and/or response personnel.</li> <li>Emergency medical service (EMS) dispatchers and ambulance response units.</li> <li>Fire fighter dispatchers and response personnel.</li> <li>Hazardous material control centers and other agencies offering remote diagnostic information and advice on how to respond to requests for emergency aid.</li> <li>Trauma centers and similar emergency hospices.</li> </ul> <p>Standards should be supported to address interconnection issues between PSAP and CMRS, cable television service providers.</p> <p>Media and Repair Link Redundancy/Diversity - the redundancy and diversity concepts set forth in Best Practice 6-5-0566 also should be applied to network links considered vital to a community's ability to respond to</p>

	<p>emergencies. Types of links that are critical to the provision of emergency aid during such events include communication links from the PSAP location to broadcast media organizations and local network provider repair centers.</p> <p>Media organizations can alert the public during periods of emergency network degradation or outage through appropriately worded public service. In addition, dedicated network links and/or alternate accesses to network provider repair personnel will ensure that interruptions are known immediately and that repair personnel are mobilized expeditiously.</p>
6-5-0566	<p>Diverse Interoffice Transport Facilities - When all 911 circuits are carried over a common interoffice facility route, the Public Safety Answering Point (PSAP) has increased exposure to possible service interruptions related to a single point of failure (e.g., cable cut). The 911 circuits should be placed over multiple, diverse interoffice facilities.</p> <p>Diversification may be attained by placing half of the essential communication circuits on one facility route, and the other half over another geographically diverse facility route (i.e., separate facility routes).</p> <p>Option 1: Diverse Interoffice Transport Facilities with Standby Protection - A variation of the facility diversity architecture is deployment of a 1-by-1 facility transport system. This architecture is protected by a standby protection facility that is geographically diverse from the primary facility. Because no calls are lost while switching to the alternate transport facility during primary route failure, this architecture is considered self-healing.</p> <p>Option 2: Diverse Interoffice Transport Facilities Using Digital Cross-connect System (DCS) - Earlier NRC Focus Group recommendations suggested using diverse interoffice transport facilities from the called serving end office via two diverse DCS. This approach provides diversity and, due to the concentration by the DCS network elements, offers a less costly network solution.</p> <p>Option 3: Fiber Ring Topologies for 911 Circuits - Fiber optic network elements offer network service providers the ability to aggregate large amounts of call traffic onto one transport facility. Traffic aggregation opposes the diverse facility transport recommendations defined in this document. However, fiber rings permit a collection of nodes to form a closed loop whereby each node is connected to two adjacent nodes via a duplex communications facility. Fiber rings can provide redundancy such that services may be automatically restored (self-healing), allowing failure or</p>

	<p>degradation in a segment of the network without affecting service. Bi-directional fiber rings are used in some metropolitan areas, ensuring essential communications service is unaffected by cuts to fibers riding on the ring. Ring features and functionality are part of the Synchronous Optical Network (SONET) technical requirements. When essential communications is placed on self-healing SONET rings, service interruptions are minimized due to the architecture employed. This is only true so long as single points of failure do not negate the architectural redundancies.</p> <p>Examples of single points of failure include bi-directional rings within the same route, transport, facility etc.</p>
6-6-5078	<p>Service Providers and Network Operators should consider establishing and ensuring dual transmission of all sensitive alarms and reliability of all communications links between the areas of critical infrastructure and monitoring stations in order to prepare for possible communication failures during emergency or disaster situations.</p>
6-6-1007	<p>Service Providers, Network Operators and Equipment Suppliers should consider establishing a geographically diverse back-up Emergency Operations Center.</p>
6-6-1033	<p>Network Operators should develop a strategy for employment of emergency mobile assets such as Cellular on Wheels (COW), Cellular Repeater, Switch on Wheels (SOW), Transportable Satellite Terminals (RF equipment), Microwave, Power Generators, HVAC, etc. for emergency deployment and service augmentation.</p>
6-5-0570	<p>Intraoffice 911 Termination to Mobile PSAP - Commonly, the transport facility between the PSAP and the serving end office may not have facility route diversity. To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks at the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency.</p> <p>Some PSAPs have prearranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to the LECs' end office and to connect to an RJ-11 jack for 911 call interception. Another type of receptacle may be pre-installed in the end office for connection to a mobile PSAP.</p>
6-5-0571	<p>Dual Active 911 Tandem Switches - Dual active 911 tandem switch architectures enable circuits from the callers serving end office to be split between two tandem switches. Diverse interoffice transport facilities further enhance the reliability of the dual tandem arrangement. Diversity is also deployed</p>

	<p>on interoffice transport facilities connecting each 911 tandem to the PSAP serving end office.</p>
<p>6-5-0572</p>	<p>Traffic Operator Position System (TOPS) as a 911 Tandem Backup - Operator services tandem switches can also serve as backup and/or overflow for network elements, due to their ubiquitous connectivity throughout the telephone network. In most instances, existing trunking and translations may be used when adding a TOPS to the 911 network.</p> <p>When an interoffice transport facility fails or an all-trunks-busy condition occurs, the backup/overflow route to the operator services tandem is selected. The operator tandem switch recognizes the call as an emergency by translating the 911 dialed digits, and may be preprogrammed to automatically route the call to the serving 911 tandem switch.</p> <p>Further, if the operator tandem switch is unable to access the 911 tandem switch, the call will automatically be "looped around" so that an operator may manually answer the call and manually attempt to reach an emergency services provider.</p>
<p>6-5-0658</p>	<p>Maintain adequate fuel on-site and have a well-defined re-supply plan. Improve fuel systems reliability by providing redundant pumps for day tanks and a manual-priming pump. Wherever possible, use dual-source generators with direct line natural gas as the primary and liquid fuel (normally diesel) as a backup to provide a long-term fuel source in times of long power outages.</p>
<p>6-5-0690</p>	<p>Redundancy must be provided, so that no single point alarm system failure will lead to a battery plant outage.</p>
<p>6-5-0569</p>	<p>Option 1: PSTN as a Backup for 911 Dedicated Trunks - To ensure that 911 is minimally affected by potential traffic congestion sometimes experienced in the PSTN, PSAPs commonly create dedicated private public safety networks. A low-cost alternative for handling 911 calls during periods of failure in the end office-to-911 tandem transport facility, is to use the PSTN as a backup between the caller's end office and the 911 tandem switch. Such applications may or may not make use of adjunct devices that monitor primary trunk path integrity.</p> <p>If the primary path to the 911 Tandem switch should be interrupted or all-trunks-busy, the call may be forwarded over the PSTN to a preprogrammed directory number. Further, the caller may be identified if the administrative line is equipped with a caller identification (ID) device.</p> <p>Option 2: Wireless Network as Backup for 911 Dedicated Trunks - Similar to the PSTN backup for completing 911</p>

	calls when the primary transport facility is interrupted, wireless networks may provide more diversity than the PSTN alternative.
<b>Contingency/Emergency Planning</b>	
6-5-0574	Network Management Center and Repair Priority - Network Management Centers (NMCs) should remotely monitor and manage the 911 network components. The NMCs should use network controls where technically feasible to quickly restore 911 service and provide priority repair during network failure events.
6-6-3202	The Service Provider and the Public Safety Agency or its agent, that utilize an Emergency Notification System (Public Safety Mass Calling) should have a pre-established procedure to notify all impacted network operators, prior to launching an alert event. This process will reduce the potential of switch overload and resultant call blocking that may impact emergency and other essential services.
6-6-3212	Service Providers and Network Operators should provide training for their operations personnel on network-level trouble shooting. Network Operators and Service Providers should proactively include Public Safety Service and Support providers when developing trouble reporting plans and subsequent training.
6-6-0513	Service Providers and Network Operators should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration for inter-connected networks. Where appropriate, this information should be shared with Public Safety Service and Support providers. The NIIF web site is <a href="http://www.attis.org/atis/clc/niif">http://www.attis.org/atis/clc/niif</a> .
6-6-0577	<p>911 Contingency Plan Training - Once a contingency plan is developed, it should be periodically tested. These tests can be of various types:</p> <ul style="list-style-type: none"> <li>desktop check tests (using a checklist to verify familiarity of "what to do in case of"),</li> <li>procedures verification test (verify that established procedures are followed in a simulation),</li> <li>simulation test (similar to a fire drill, e.g., simulating a disaster and monitoring the response),</li> <li>actual operations test (cause an event to happen, e.g., power or computer failure and monitor the response),</li> <li>actual security checks to verify the security of the essential service nodes (e.g., access controls to the ALI and MPC databases).</li> </ul> <p>The importance of testing a contingency plan is critical to its success. An annual schedule of testing and evaluating written results is an excellent method of ensuring that a plan will work in the event of a disaster and for identifying weaknesses in the plan.</p>

	<p>Close cooperation between a Service Provider and the PSAP in conducting actual operations testing will be of mutual benefit to both the Service Provider and the PSAP. An annual comprehensive operational test of the contingency plan is strongly encouraged.</p>
<p>6-6-0586</p>	<p>Service Providers of critical services to National Security and Emergency Preparedness (NSEP) users should avail themselves of the Telecommunication Electric Service Priority (TESP) restoration initiative. The TESP initiative helps to ensure relatively stable NSEP communications by enabling utility companies to efficiently identify critical national, state, and local NSEP telecommunications facilities that qualify for priority restoration of electric service. Therefore, by participating in the TESP initiative, telecommunications Service Providers, utility companies, and state organizations and Public Safety Service and Support organizations collectively serve to ensure that essential national defense and civilian requirements are met. More information on the TESP initiative can be obtained from the National Communications System (NCS) Office of Priority Telecommunications, Manager National Communications System, Attn: OPT/N3, 701 South Courthouse Road, Arlington, Virginia 22204-2198, on telephone 703-607-4932 or email at TESP@NCS.GOV.</p>
<p>6-6-0599</p>	<p>Test a Network's Operational Readiness through planned drills or simulated exercises. Service Providers should conduct exercises periodically keeping the following goals in mind:</p> <p>The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible. While the staff must be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified. Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service. It is particularly important to coordinate disaster exercises with other Service Provider, Public Safety Providers and vendors. It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.</p>
<p>6-6-0619</p>	<p>All Service Providers and Public Safety Providers should develop and/or ensure that appropriate pre-plans with fire agencies exist for all equipment locations and provide</p>

	automatic notification to local fire department.
6-6-0655	Service Providers and electric utilities should plan jointly to coordinate hurricane and other disaster restoration work. Service Providers should proactively include Public Safety Service and Support Providers when developing disaster restoration and prioritization plans.
6-6-5031	Service Providers, Network Operators and Equipment Suppliers should establish a definitive role for security in business continuity planning, including emergency response plans (e.g., a 24 hour and 7 day-a-week emergency notification procedure) and periodic tests of such plans.
6-6-5093	Service Providers, Network Operators, Equipment Suppliers and Property Managers should establish, implement and test emergency response and crisis management programs to include external first responders and civic authorities in mutual emergency preparedness planning, as appropriate (e.g., on-site visits, access to facilities, mutual familiarity with plans and procedures, single points of contacts). First responders may include Emergency Response Team (ERT), law enforcement, fire department, FEMA, NS/EP, DHS, etc.
6-6-5226	Service Providers, Network Operators and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to ensure effective coordination for emergency response and restoration.
6-6-1003	The Business Continuity Plan for Service Providers and Network Operators should address critical business processes (e.g., Call Completion, 911/Emergency Services, Provisioning, Maintenance, etc.), support functions (IT, Sourcing, Logistics, Real Estate, etc.) and key business partners.
6-6-1006	Service Providers, Network Operators and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.
6-6-1035	Disaster Recovery exercises should include trial deployment of emergency mobile assets and should be conducted to train as many technicians and support personnel as possible in as realistic a manner as possible.
6-6-1057	Service Providers, Network Operators, and Equipment Suppliers should ensure deployment of Government Emergency Telecommunications Service (GETS) cards to appropriate Disaster Recovery personnel. Appropriate training and testing should be provided as necessary.

6-6-1063	All Service Providers and Network Operators should set Initial Address Messages (IAMs) to congestion priority level 0 for all POTS calls. This will ensure government emergency calls ( 911, GETS ) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111. The Network Interconnection Interoperability Forum (NIIF) ( <a href="http://www.atis.org/atis/clc/niif/pots.htm">www.atis.org/atis/clc/niif/pots.htm</a> ), is tracking implementation as part of NIIF Issue 0095 in coordination with the Office of the Manager, National Communications System.
6-5-0598	Develop crisis management exercises - Service Providers should, at a minimum, have a communications structure in place for timely notification of affected parties in the event of disasters or emergencies. During the past several years a number of disastrous events have prompted an increased awareness on the part of all members of the telecommunication industry to the critical need to have a Disaster Preparedness strategy. This strategy should outline a network Service Provider's Disaster Preparedness organization, the roles, responsibilities and training of its members and provide for cooperative interaction among both internal and external organizations. The purpose of this strategy is to provide for the development of emergency plans that protect employees, ensure service continuity and provide for the orderly restoration of critical services in the event of a major network catastrophe.
6-5-0587	Users, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NSEP) users should avail themselves of the Telecommunications Service Priority (TSP) priority restoration for critical facilities. The TSP Program is a FCC program used to identify and prioritize telecommunication services that support NSEP missions. The TSP Program also provides a legal means for the telecommunications industry to provide preferential treatment to services enrolled in the program. More information on the TSP Program can be obtained from the National Communications System (NCOS) Office of Priority Telecommunications, Manager National Communications System, Attn: OPT/N3, 701 South Courthouse Road, Arlington, Virginia 22204-2198, on telephone 703-607-4932 or email at <a href="mailto:TESP@NCS.GOV">TESP@NCS.GOV</a> .
6-6-1062	Service Providers and Network Operators should establish and maintain an interface with local, state, and federal government agencies to ensure effective support is available upon request as part of disaster recovery.
6-6-1052	Service Providers and Network Operators should periodically test new and existing business critical systems for capability limitations to avoid impaired operation during disasters.

6-6-1045	Service Providers and Network Operators should develop a plan or process so resource needs, identified through damage and resource assessments, can be escalated up the company chain of command, with vendors, or through mutual-aid partners.
6-6-1020	Service Providers, Network Operators, and Equipment Suppliers should identify the need for Chemical Biological Radiological Nuclear (CBRN) response via internal hazardous material response team or contracting with an external HazMat response and remediation vendor to be able to safely respond to the aftermath of a Weapons of Mass Destruction (WMD) attack.
6-6-1023	Service Providers, Network Operators, and Equipment Suppliers should identify key individuals within their organizations that are critical to disaster recovery efforts. Planning should consider maximizing the availability of these individuals.
6-6-1025	Service Providers and Network Operators should consider creating a threat assessment team to quickly determine appropriate actions both pro-active or re-active to address potential or real threats.
6-6-1031	Service Providers and Network Operators should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. ( <a href="http://www.ncs.gov/ncc/main.html">www.ncs.gov/ncc/main.html</a> and <a href="http://www.nric.org/meetings/meeting20020913.html">www.nric.org/meetings/meeting20020913.html</a> )
6-6-1009	Service Providers, Network Operators and Equipment Suppliers should regularly exercise their Disaster Recovery Plans. Exercise scenarios should include natural and man-made (e.g., nuclear, biological, and chemical) disasters.
6-6-1010	Service Providers, Network Operators and Equipment Suppliers should designate personnel responsible for maintaining the Disaster Recovery Plans.
6-6-1012	Service Providers, Network Operators and Equipment Suppliers should develop company specific protective measures that correlate with the threat levels identified in the Homeland Security Advisory System
6-5-0613	A number of outages are of extended duration because the technician does not have the spare equipment, tools nor test equipment to implement the restoration. The most common cause is unavailability of spare circuit cards/packs. This results in a delay until the spares are located and shipped from some other location. To prevent these delays, a process should be established to track the location of all spare equipment. This process should align with network performance and reliability requirements and should include procedures for allocating, procuring, delivering, and deploying spare equipment. When spares are not locally available, the process should also provide a method to expedite identification and delivery of the required

	equipment.
<b>Data Assurance/Traffic Management</b>	
6-6-0575	<p>Diverse Automatic Location Identification used in Public Safety, like ALI (Automatic Line Identification) and MPC (Mobile Positioning Center) systems should be deployed in a redundant, geographically diverse fashion (i.e. two identical ALI/MPC data base systems with mirrored data located in geographically diverse locations).</p> <p>To improve ALI/MPC reliability, deployments of fully redundant Public Safety database systems, such that ALI/MPC system hardware and/or software failure does not impair ALI/MPC data accessibility, will further improve ALI/MPC reliability. When deployed with geographically diverse transport facilities, single points of failure may be eliminated.</p> <p>ALI/MPC data should be placed on fault-tolerant and secure computer platforms to increase the reliability of ALI/MPC display retrievals. When possible, "hot spare" computers should be held in reserve for catastrophic events.</p>
6-5-0585	<p>Service Providers, Equipment Suppliers and representatives of the National Security and Emergency Preparedness (NSEP) community should work together to share information regarding security issues related to packet network convergence with the PSTN, including identification and authentication procedures for emergency calls, and issues related to cyber attacks and malicious intrusion into networks.</p>
6-5-0758	<p>If 911 call completion is affected, test calls should be made by the Service Provider to the PSAP(s) to assess the impact. Once service is restored, the Service Provider should make multiple 911 test calls to ensure they complete properly.</p>
6-6-0802	<p>Equipment Suppliers should incorporate traffic management technology into their equipment, as necessary, with the tools necessary to maintain performance of facilities and to manage traffic flows from customers per contracts/SLA's and to prevent degradation of quality of service experienced by network users.</p>
6-6-0803	<p>Service Providers, Network Operators and Equipment Suppliers are encouraged to continue to participate in the development and expansion of industry standards for traffic management that promote interoperability and assist in meeting end user quality of service needs.</p>

6-5-0581	<p>Private Switch (PS)/ Alternative LEC (CLEC) ALI -- ALI data for alternate providers (e.g., PS, CLEC) should be included in the ALI systems.</p> <p>PSAPs have become increasingly reliant on the ALI data administered by the LECs, and believe that those individuals served by private telecommunication providers and/or alternate LEC providers should have their address information contained in their ALI data base systems. The NENA Recommended Formats for Data Exchange and the NENA Recommended Protocols for Data Exchange were established to enable ALI data integration of these providers.</p>
6-6-1061	<p>Service Providers, Network Operators, and Equipment Suppliers should ensure that Telecommunication Service Priority (TSP) records and data bases are reconciled annually.</p>
<b>Media/Public Awareness</b>	
6-5-0576	<p>Move Mass Calling Stimulator away from 911 Tandem Switch - Mass calling events may cause 911 service interruptions. Service interruptions caused by media stimulated calling has prompted the LECs to reassess and improve the handling of mass calling events. The 911 Tandem switch serves as the most critical network element in providing 911 service. If a media stimulated mass calling event is served by a 911 Tandem, the PSAPs being served by the 911 Tandem may experience delayed dial tone when call transfer is attempted by the PSAP personnel. The PSAP may also experience delays in call completion (ring-back tone) or a fast busy signal, which indicates that the call has failed to complete. To mitigate such instances, high volume call events should be moved to another end office.</p> <p>Pre-Planning for Mass Calling Events - To minimize the potential of interruption caused by media driven mass calling events, the LEC can identify periods of low call volume traffic so that the media may schedule mass calling events during low traffic periods.</p> <p>Carrier external affairs and marketing groups should work closely with media organizations to ensure 911 callers are unaffected by mass calling events.</p>
6-5-0578	<p>Educate the public on proper use of essential communications - The public's proper use of 911 service is critical to the effectiveness of the emergency network's operation. Misuse of 911 could lead to the following: congestion of the 911 network, leaving callers with real emergencies unable to contact a 911 operator, exhaustion of resources on non-emergency situations, reduction in a jurisdiction's ability to respond to emergency situations in a timely manner because of the jurisdiction's emergency response agencies being overwhelmed by responses to non-emergency situations. This could have potentially disastrous effects on the public's perception of its</p>

	emergency network and emergency response agencies.
6-5-0582	Commercial Mobil Radio Services (CMRS) - Emergency Calling - The CMRS industry should consider 911 as the standard access code for emergency services (e.g., law enforcement, fire, EMS, hazardous materials). Implementation of such a standard would eliminate confusion among mobile communications users when they are in a roaming mode.
6-6-3201	Commercial TV and radio broadcasters should work with Public Safety organizations (PSAPs) to have a disaster recovery action in place in the event of a commercial communications failure effecting their 911 network, to inform callers requiring emergency services that they should dial a 7/10 digit number to reach PSAP administrative lines.
6-6-3204	Service providers should work with Public Safety Service and Support providers to educate the public on the proper use of N11 Access codes (211, 311 and 511 services) such that it enables the 911 network and personnel to be exclusively focused on emergencies. Proper use of all N11 codes, including 911, prevents exhaustion of resources of emergency personnel on non-emergency situations. (Reference NRIC BP 6-5-0578)
6-6-3203	To assist in the effectiveness of Emergency Notification Systems (Public Safety Mass Calling) and return calls from PSAPs, Service providers should consider developing options that allow for call delivery from Emergency Notification Services to subscribers with call blocking/screening services.
6-6-3209	Where practical, CATV facilities shall receive signals from off-air broadcasters via fiber as the primary source with automatic fail over to the off-air signal as the secondary source.
6-6-3210	Where practical, CATV service providers should serve Emergency Operations Centers with a CATV connection to provide video for viewing local weather and news information, a diverse connection to the Internet and a diverse telecommunications connection if such services are available on the network.
<b>Emergency Management</b>	
6-6-5267	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that standard operating procedures are clearly defined, reinforced, and followed by personnel during emergency situations in order to avoid degradation of security due to a diversion.
6-6-1018	Service Providers, Network Operators, and Equipment Suppliers should always emphasize employee and public

	safety during all phases of disaster recovery.
6-6-1008	Incident coordination and control in the emergency operations center and at the incident site should be achieved through the use of the Incident Command System (see National Fire Protection Association (NFPA) Standard 1561.
6-6-1037	Service Providers, Network Operators, and Equipment Suppliers should consider using a disaster recovery support model with escalation procedures that provide a clear escalation path to executive levels both internally and externally.
6-6-1038	Service Providers, Network Operators and Equipment Suppliers should consider during times of disaster, communicating the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response.
6-6-1011	Service Providers, Network Operators and Equipment Suppliers should consider utilizing multiple alternative communication devices and service providers for critical service personnel during emergencies.
6-6-1016	Service Providers and Network Operators should develop processes or plans to quickly account for all employees (e.g. field techs) in or near the impact area of a disaster.
6-6-5266	Service Providers, Network Operators, Equipment Suppliers and Property Managers personnel should be made aware that information of an event that directs emergency resources might be a terrorist or criminal diversion.
<b>Prevention</b>	
6-5-0737	As new network elements are introduced, consideration should be given for the need to implement other NRIC Network Element Best Practices. For example, as transport network elements take on more network control, additional Best Practices become applicable.
6-6-5131	Network Operators should provide appropriate security for emergency mobile trailers (both pre- and post-deployment) in order to protect against a coordinated terrorist attack on emergency communications capabilities.
6-5-0567	Red-Tagged Diverse Equipment - Depending on LEC provisioning practices, the equipment in the central office can represent single points of failure. 911 circuits should be spread over similar pieces of equipment, and each plug-in-level component and frame termination should be marked with red tags. The red tags alert LEC maintenance personnel that the equipment is used for critical, essential services and is to be treated with a high level of care.

6-5-0568	<p>Option 1: Alternate PSAPs from the 911 Tandem Switch - A common method of handling PSAP-to-Tandem transport facility interruptions is to program the 911 tandem switch for alternate route selection. If the 911 caller is unable to complete the call to the PSAP, the tandem switch would automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAP's pre-arranged needs.</p> <p>Option 2: Alternate PSAPs from the Serving End Office - Another method of handling PSAP-to-Tandem transport facility interruptions is to program the end office for alternate route selection. If the 911 caller is unable to complete the call to the PSAP, the end office may automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAP's pre-arranged needs.</p>
6-6-5129	<p>Service Providers who are required by the government to file outage reports for major network outages should ensure that such reports do not unnecessarily contain information that discloses specific network vulnerabilities, in order to prevent such information from being unnecessarily available in public access.</p>
6-5-0540	<p>Equipment Suppliers should share countermeasures resulting from analysis of an outage with Network Operators using the same equipment.</p>
6-6-1019	<p>Service Providers, Network Operators, and Equipment Suppliers should maintain their participation in NRIC which includes advisory sessions, exercises, and training. They should review existing and proposed best practices and consider implementation.</p>
6-5-0548	<p>Network Operators should conduct their own failure data collection and analysis procedures to perform root cause analysis. Network Operators and Equipment Suppliers should work together to jointly perform this analysis and implement corrective measures. For insights into categorization of outages, see the NRSC outage analysis categories.</p>
6-5-0583	<p>Outage Reporting - All Service Providers should have a uniform method of reporting and tracking significant service outages for internal use and, where required, for outage reporting to the FCC. Root cause analysis, publication of results and new best practices may be left up to the industry.</p>

6-5-0591	Information sharing guidelines - Industry guidelines for the sharing of information about network outages is included in the NIIF Reference Document Part VII. This document is intended to provide the appropriate guidance to facilitate the sharing of information. It identifies types of information which may be shared, the circumstances under which it should be shared, the extent to which sharing is appropriate, and the mechanisms and timing for that sharing. It represents industry consensus arrived at with the full participation of members of the Network Interconnection Interoperability Forum (NIIF) which consists of Access Service Providers, Access Service Customers and Vendor/Manufacturers. The NIIF documents are available at <a href="http://www.atis.org/atis/clc/niif">http://www.atis.org/atis/clc/niif</a> .
6-5-0593	Outage information sharing - A prime source for information concerning outages is the network outages reported to the FCC as required by Section 63.100 of the rules. Review of the reports at <a href="http://www.fcc.gov/oet/outage">http://www.fcc.gov/oet/outage</a> will enable the reader to become aware of significant problems impacting network services.
6-5-0561	Documentation should be developed with a clear understanding of customers' expectations and needs; Service Provider input and human factors consideration are essential. Documentation should be produced in a complete, easy-to-use, and timely manner. It should be made accessible to the entire customer base. The use of electronic media to maintain the documentation manuscripts and to access customer distribution information is essential. The operations and maintenance manual should give an overview of the system and identify procedures for regularly scheduled operations, including security administration (ref. GR-815, GR-1332, NIIF) and should cover methods to recover from total and partial network element outages. In addition, the documentation should be clear on how to manage emergency and unforeseen situations, including a technical support escalation process. These plans should be made available to each other and should converge so both parties have clear expectations when these problems arise in the network. Escalation strategies should be continuously reviewed for effectiveness based on field performance. "GR" stands for Generic Requirements published by Telcordia ( <a href="http://www.telcordia.com">http://www.telcordia.com</a> ) and the NIIF ( <a href="http://www.atis.org/atis/clc/niif">http://www.atis.org/atis/clc/niif</a> ).
6-5-0738	Track and analyze facility outages. Take action if any substantial negative trend arises or persists.
6-6-0801	Service Providers should consider utilizing traffic management mechanisms and technologies to ensure facilities are utilized most efficiently.

6-6-0802	Equipment Suppliers should incorporate traffic management technology into their equipment, as necessary, with the tools necessary to maintain performance of facilities and to manage traffic flows from customers per contracts/SLA's and to prevent degradation of quality of service experienced by network users.
6-6-0803	Service Providers, Network Operators and Equipment Suppliers are encouraged to continue to participate in the development and expansion of industry standards for traffic management that promote interoperability and assist in meeting end user quality of service needs.
6-6-1060	Service Providers, Network Operators and Equipment Suppliers should work with Federal and State legislators and regulatory bodies to enact stricter laws and ordinances regarding back-hoe fades and related cable cuts.
6-6-0512	Service Providers and Network Operators should perform periodic inspection of cable ways (e.g., through floor and through wall passage ways, sealing compounds, fire and water stopping, etc.). Public Safety Service and Support providers should also perform these inspections at their communication centers.
<b>Cooperation/Communications with Emergency Service Entities</b>	
6-6-1059	Service Providers should work with government and other utilities in the development of State Emergency Communications Networks in order to provide a process for key utilities and government emergency responders to communicate during disaster events.
6-6-3211	Network Operators and Service Providers should develop and maintain operations plans that address network reliability issues. Network Operators and Service Providers should proactively include Public Safety Service and Support providers when developing network reliability plans.
6-6-3213	Service Providers, Equipment Suppliers and Public Safety Service and Support providers should work together to establish reliability and performance objectives in the field environment.
6-5-0505	When required by law, Network Operators and Service Providers should have procedures in place to support wire taps for court orders, or for other appropriate reasons (e.g., property rights protection from harmful activity).
6-5-0724	Improve the effectiveness of state One-Call legislation.
6-5-0725	Increase stakeholder coordination and cooperation on state one-call legislation efforts.
6-5-0732	Take an active role on One-Call Board and solicit information from other stakeholders.
6-5-0740	Conform to the Minimum Performance Guidelines for One-Call Notification Systems.
6-5-0743	Ensure that federal one-call legislation is used to bring all states up to high level of damage prevention.

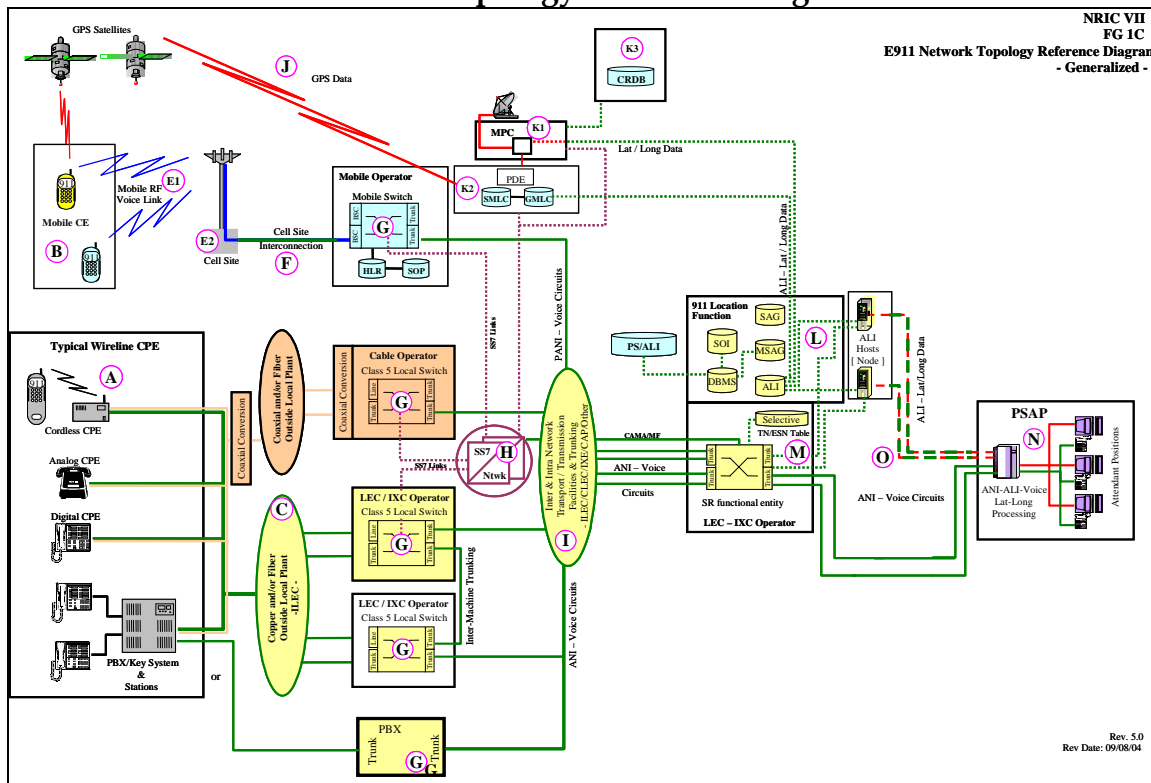
6-5-0579	<p>Improve communications among all Service Providers and PSAPs - Service Providers, 911 administrators, and public safety agencies should continually strive to improve communication among themselves. They should routinely team to develop, review, and update disaster recovery plans for 911 disruption contingencies, share information about network and system security and reliability, and determine user preferences for call overflow routing conditions.</p> <p>They should actively participate in industry forums and associations focused on improving the reliability and security of emergency services and the development of technical industry standards. The National Emergency Number Association (NENA) and the Association of Public-safety Communications Officials (APCO) are two of the organizations that are open to all stakeholders of 911 service delivery and that are focused on finding 911 solutions for emerging technologies (e.g., wireless, PBX, CLEC).</p>
6-6-5071	<p>In order to prepare for contingencies, Service Providers, Network Operators and Property Managers must maintain liaison with local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.</p>
6-5-0584	<p>Service Providers, Network Operators and Equipment Suppliers and representatives of the National Security Emergency Preparedness (NSEP) community should work together to support appropriate industry and international organizations to develop and implement NSEP features and functionality in packet networks.</p>
6-6-1058	<p>Service Providers and Equipment Suppliers should work collectively with local, state, and federal governments and other utilities to develop a process for efficient communications and coordination.</p>
6-6-1021	<p>Service Providers, Network Operators, and Equipment Suppliers should provide disaster recovery contact information to the National Coordinating Center (NCC) and update this contact information as changes occur or at the direction of the NCC.</p>

### 5.3 Architecture Vulnerabilities

#### 5.3.1 911 Network Topology Reference Diagram

A Reference Diagram was developed to “level-set” the team when assessing the architecture vulnerabilities. As such, FG 1C set about assembling a reference diagram that illustrates a high-level, common network architecture. This reference diagram is a graphic illustration of network components and architectures that will facilitate analysis by allowing the team to compare “apples to apples” when dealing with differing technologies and functionalities. A larger version of the below reference diagram can be found in Appendix I.

Exhibit 5.3.1 - 911 Network Topology Reference Diagram



#### 5.3.2 Summary of Findings

In reviewing the key components of the 911 network and the outage data, we believe that the most vulnerable areas of the network are:

- Vulnerability #1, Facility- affected by 47% of the 911 outages
- Vulnerability #2, Power Elements - affected by 16% of the 911 outages
- Vulnerability #3, CCS - affected by 14% of the 911 outages
- Vulnerability #4, Local Switch, affected by 9% & Tandem Switch - affected by 4% for a total 13% of the 911 outages
- Vulnerability #5, DCS, - affected by 7% of the 911 outages

### 5.3.3 E911 Network architecture areas most impacted by outages

#### Vulnerability #1: Facility

##### Single Points of Failure

In reviewing the outage data, it appears that single points of failure still plague the 911 network. Best practices of diversity, redundancy, and adoption of policies of dual network facilities for critical infrastructure are not universally employed. One would expect that, at least in urban areas where many of the outages occurred, significant options are generally available to deploy more robust network elements. As technologies advance and increase the reliability of networks and network elements it would seem that single failure points should become a design element of the past. However, today, single failure points continue to exist and create problems for 911 networks.

##### Unprotected Fiber

Many of the 911 outages reported in the analysis period from January of 2002 through the first quarter of 2004 demonstrate the vulnerability of unprotected fiber portions of the 911 network. Cable cuts caused by inaccurate locates of buried fiber by the service provider or no locate of buried fiber requested by contractors contribute to a significant portion of the total outages. It was noted by one of the participants that the use of fiber optic cable for telecommunications transmissions has a tendency to concentrate signaling due to its capacity and ease of use. Buried fiber is also more difficult to field locate than the bundles of copper.

There are Best Practices in place to help mitigate outages of this nature, and we believe increased attention to this critical element should be considered.

#### Vulnerability #2: Power Elements

##### Redundant Power

Analysis reveals that lack of redundant power for essential hardware elements (such as DACS) contributes to current outage experiences. Again, these are high capacity concentration points that appear to create opportunities for single points of failure. Environmental situations such as fire, flood, and lightning can all cause the loss of commercial power either at the public safety answering point or in a critical component of the service provider network, such as the MPC or a central office. Lack of redundant power in any of these situations can adversely affect the continuity of operations.

### Vulnerability #3: CCS

While it would appear that the vulnerability identified can be categorized as a CCS failure, in reality the failure may be with the lack of application of some of the important Best Practices related to network design that can also be applied to this network element. There are Best Practices in place addressing diversity that can be specifically applied to address this vulnerability. Examples include:

- Employment of dual network elements deemed to be critical infrastructure
- Auditing of diversity on a regular basis to ensure optimum levels are maintained over time
- Maintaining link diversity

### Vulnerability #4:

#### Local Switch--Host / Remote Configurations

Host / Remote configurations are sometimes employed in a network where a service provider is limited in facilities or resources. While this is a viable solution in some limited application, Host/Remote configurations where there is no diversity in the umbilical facilities expose the network to considerable vulnerability. Wherever possible, diverse umbilical facilities should be utilized. Where no diversity for the remote exists, alternate means of employing diversity should be explored. Although there is an existing best practice addressing this issue, it is unclear to what extent this Best Practice is being followed.

#### Tandem Switch

The vulnerabilities associated with the 911 network tandem switch are similar in nature to those vulnerabilities discussed above. Preventative measures such as dual switches, redundant power, and diversity in critical network elements, if deployed, can reduce the number of outages related to tandem switches.

### All Vulnerabilities: Incorporating Best Practices into Processes & Procedures

Understanding and applying existing NRIC Best Practices may be the best opportunity to diminish the vulnerability to 911 networks and reduce related outages. We note that in many of the outages reviewed in the analysis, the problem was not that a Best Practice was not identified to prevent the outage situation, but that the identified Best Practice was not followed. In many cases the carrier noted multiple Best Practices which, if followed, could have precluded the outage. It is recommended that companies consider incorporating Best Practices aimed at mitigating vulnerabilities.

Best Practices should also be followed by public safety entities. NRIC V and VI appropriately provided guidance to public safety with regard to Best Practices that fell within the purview of public safety jurisdiction. Education of public safety entities on the applicable Best Practices related to network design, standards, ongoing observance to maintenance, components within and under the control of the public safety entity should be encouraged. Although the Best Practices are typically carrier deployed, there is a clear role for public safety to assure that the deployment occurs and that regular audits occur to assure that the deployed redundant or diverse facilities are maintained.

## **6 Next Steps**

With the completion of the identification of Best Practices related to E911 outages as well as the identification of key network vulnerabilities, the next step for Focus Group 1C will be to develop and administer a survey to determine how effective Best Practices have been for emergency communications. The results of this survey will be reported to the Council, per the NRIC VII Charter, by June 24, 2005.

Once the survey results are obtained, they will be analyzed and applied to the existing Best Practices in an effort to refine the language to better assist in the prevention of E911 outages. A gap analysis of the existing Best Practices will be performed to identify areas where new Best Practices may be required. Finally, any new Best Practices will be written.

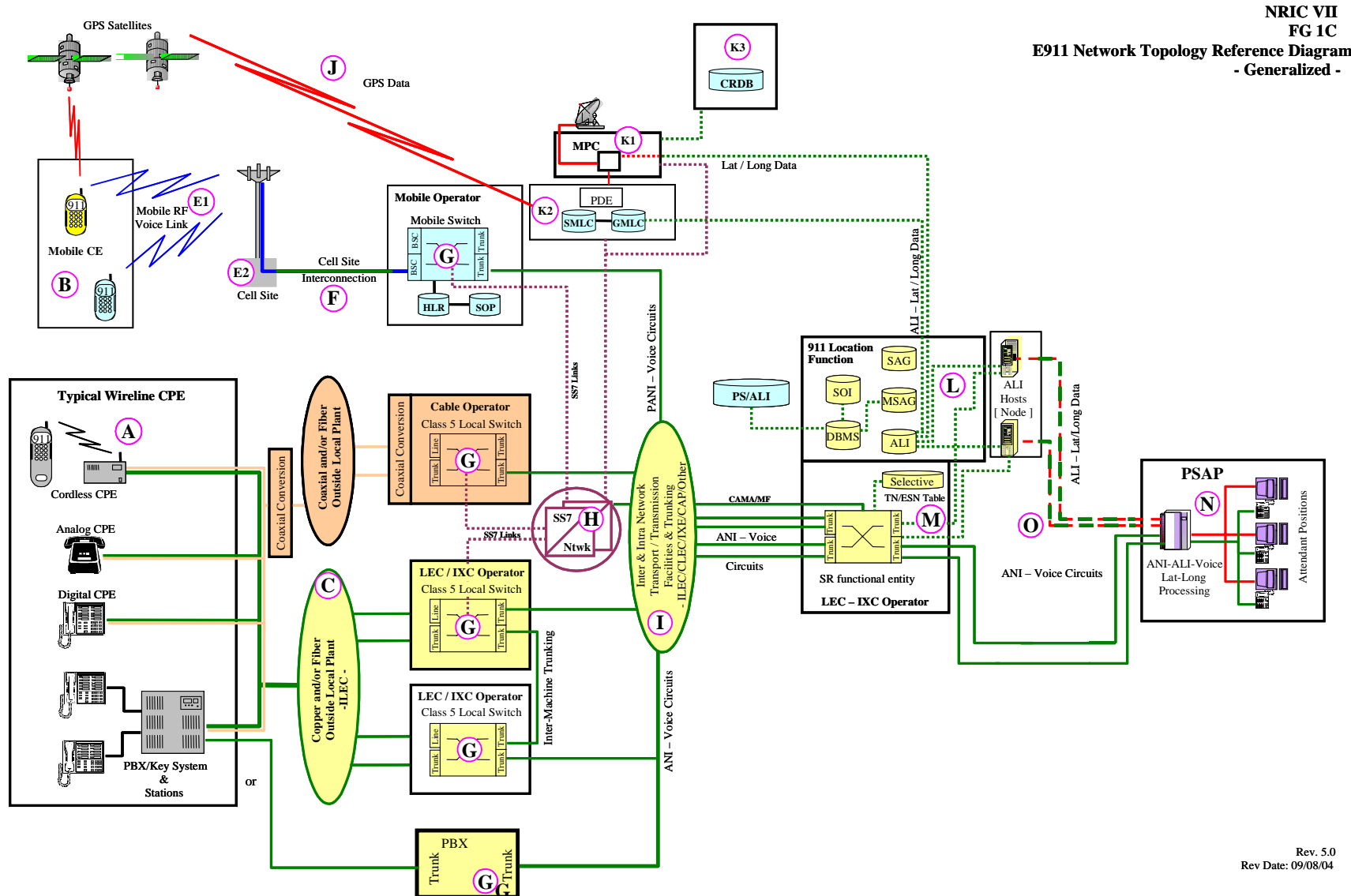
Additionally, Focus Group 1C will develop recommendations on ways to improve the relevance of the FCC-Reportable Outage data for improving Emergency Communications, including defining direct causes and root causes which are better attuned to E911. These recommendations and revised Best Practices will be provided to the Council by December 16, 2005.

## **7 Appendix 1 – Sources and Documentation**

### ***7.1 Scrubbed outage data***

See attached file entitled “FG1C\_Appendix1\_7.1\_Scrubbed Outage Data.pdf”

## 7.2 911 Network Topology Reference Diagram



NRIC VII  
FG 1C  
E911 Network Topology Reference Diagram  
- Generalized -

Rev. 5.0  
Rev Date: 09/08/04

### Network Topology Diagram Reference Point Descriptions

Reference Point	Description	Comment I	Comment II
A	Wireline CPE	Customer Premises Equipment	
B	Wireless CE	Customer Equipment	
C	LEC Operator "Last Mile" Outside Plant	LEC(Incumbent or Competitive Provider) IXC/CAP/Other Transmission Facilities	-
D	Cable Operator Coaxial Outside Plant		
E1	Mobile CE to Cell Site RF Voice Link	Mobile customer equipment transmission to cell site	
E2	Mobile Operator RF Cell Site	Cell site	Reference E2 is not to be confused with the E2 interface utilized between wireless network and 911 service provider
F	Cell Site to Mobile Switch Backhaul	LEC(Incumbent or Competitive Provider) IXC/CAP/Other Transmission Facilities	
G	Wireline / Cable / Wireless Operator Switches	Class 5 Level Switches, PBX, or equivalent	
H	SS7 Network & Links	Reflects all operator and 3rd party provider STP's and Links	Use of SS7 signaling is optional; traditional methods utilize CAMA signaling
I	Intra & Inter Network Switching Transmission Facilities	LEC(Incumbent or Competitive Provider) IXC/CAP/Other Transmission Facilities	Class 4 Access Tandem
J	GPS Data	GPS data to PDE	Part of AGPS solution
K1	Mobile Positioning Center	Wireless Service Provider to PSAP Interface	Determines routing to the PSAP and Stages caller location data
K2	Positioning Determination Equipment (PDE) Serving Mobile Location Center (SMLC) Gateway Mobile Location Center (GMLC)	Contains RF cell site information supporting the calculations for determining caller location data	
K3	Coordinate Routing Data Base	Database providing routing instructions on wireless call utilizing latitude & longitude translated to routing table for appropriate PSAP based on location data	
L	Wireline Operator E911 Location Function	Traditional E911 data processes supporting location information provided to PSAP on wireline 911 call	
M	911 Service Provider Selective Router	May or may not be a telephone central office	
N	Public Service Answering Point - PSAP	Staff, Equipment, and Physical facility which performs PSAP defined responsibilities	
O	PSAP to Operator transmission link	For use only with Public Safety	
SR	Selective Router	Equipment and software providing routing functions in the traditional E911 network	
SR 2	Selective Router routing instructions	TN/ESN Table or dynamic ALI	

### ***7.3 47 C.F.R. § 63.100: Notification of Service Outage***

See the attached file entitled "FG1C\_Appendix1\_7.3\_47cfr63.100.pdf"

### ***7.4 FCC 04-188 New Part 4 of the Commission's Rules Concerning Disruptions to Communications***

See attached file entitled "FG1C\_Appendix1\_7.4\_FCC-04-188A1.pdf"

### ***7.5 NRSC Direct Cause and Root Cause Definitions***

The below definitions were taken from the Network Reliability Steering Committee's (NRSC) Outage Reporting Direct and Root Cause Definitions document. NRSC is a committee of ATIS.<sup>12</sup> These definitions were used by Focus Group 1C in identifying the direct cause and root cause categories and sub-categories that could be applied to each of the outages in the outage analysis.

## **DIRECT CAUSE**

### **Procedural - Service Provider**

#### **Failure to follow standard procedures/documentation**

Work error by service provider personnel; correct procedures exist and were generally available, but correct procedures/ documentation were not used, or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

#### **Followed procedures/documentation that were incorrect**

Flawed documentation or procedures used by service provider personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures/ documentation did not exist, or were not generally available.

### **Procedural - System Vendor**

#### **Failure to follow standard procedures/documentation**

Work error by system vendor personnel; correct procedures exist and were generally available, but correct procedures/ documentation were not used, or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

#### **Followed procedures/documentation that were incorrect**

Flawed documentation or procedures used by system vendor personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or

---

<sup>12</sup> [www.ATIS.org](http://www.ATIS.org)

typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures or documentation did not exist, or were not generally available.

#### **Procedural - Other Vendor**

##### **Failure to follow standard procedures/documentation**

Work error by other vendor personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used, or were used incorrectly. Includes use of outof-date or incorrect procedures or documentation when current or corrected documentation was generally available.

##### **Followed procedures/documentation that were incorrect**

Flawed documentation or procedures used by other vendor personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures/documentation did not exist, or were not generally available.

#### **Design - Software**

Faulty or defective software design. Includes inadequate fault recovery strategies or failures; ineffective software fault isolation performance that triggers system re-initializations, or requires manual system recovery action for resolution. Includes insufficient software/memory capacity allocation problems.

#### **Design - Firmware**

Faulty or defective firmware design. Includes inadequate fault recovery strategies or failures, and ineffective fault isolation performance that require manual recovery action for resolution. Includes problems associated with incomplete firmware restoral (with or without accurate state indicators) following re-initialization.

#### **Design - Hardware**

Faulty or defective system hardware design. Includes problems with component independence and single-point-of-failure problems between otherwise-duplex components, as well as physical hardware design problems (i.e., bad connectors, inadequate grounding techniques). If failure was the result of a product change notice (PCN) inappropriately delayed by the vendor or service provider, or the PCN was waived by the service provider, consider root cause procedural.

#### **Hardware Failure**

Random hardware failure not related to design, but due to the inherent unreliability of the system components. Includes failures of dc/dc converters or fuses embedded in switches and transmission equipment, unless the problem

was caused by the power plant. If (single) hardware failure causes loss of duplicated critical systems consider procedural or design fault. If system outage resulted from hardware failure occurring during simplex operation, consider root cause procedural if simplex mode resulted from inappropriate deferral of normal maintenance.

## **External Environment**

### **Natural (storms, lightning)**

External environmental conditions that exceed limitations documented in the vendor technical specifications. Includes direct effects of flooding, freezing, excessive temperature or rate of temperature changes. Includes outages resulting from lightning or external high voltage transients introduced into the system. If the entry of lightning into the system was caused by bonding and grounding violations, consider root cause procedural or design fault. If water damage was the result of cable pressurization failure, consider root cause procedural.

### **Man-made (vandalism, accidents)**

External man-made conditions that exceed documented (or reasonable) service provider technical specifications. Includes direct effects of water system ruptures, fires, vehicular accidents, vandalism, and explosions. If incident was the result of inadequate security precautions, consider root cause procedural.

### **Cable Damage**

Cable damage caused by dig-ups, (fiber) micro-bending, rodent damage, falling trees, etc. Includes underground and aerial cable failures associated with natural and man-made external environments. If incident was the result of faulty cable installation, or of cable locating activities, consider root cause procedural.

## **Internal Environment**

### **Water**

Entry of water into the system, including roof leaks, air conditioning leaks, excessive humidity, fire suppression activities, flooding, etc. If failure was the result of environmental systems failure (e.g., AC leaks, pressurization failures), or inadequate property management (e.g., unreasonable delay in repair or roof leak, predictable flooding), consider root cause procedural.

### **Temperature**

Excessive ambient temperatures, excessive rates of temperature change. If failure was the result of environmental systems failure, and a more effective response to the failure would have prevented/minimized impact of incident, consider root cause procedural.

### **Corrosion/contamination**

Corrosive contamination that enters the system from surrounding environment. Includes dust, airborne dirt, and smoke and/or fire suppression chemicals. If failure was the result of inadequate air filtration strategies or maintenance, consider root cause procedural or design fault.

### **Fire**

Fires within the telecommunications facility environment. Includes fires in test sets, peripheral equipment, power equipment, and building systems. If incident

was the result of service provider/others' activities, consider root cause procedural.

### **Traffic/System Overload**

#### **Reduced capacity due to system trouble**

System overload or congestion associated with decreased system throughput or trouble-caused resource limitation; does not include system congestion associated with simple high volume traffic conditions. If failure was the result of excessive out-of-service conditions, consider root cause procedural. If failure was a result of overload triggered by moderate increase in traffic/attempts, or recovery-associated activities, consider root cause design fault.

#### **High call volume**

System overload or congestion associated with high traffic or load conditions that exceed the engineered capacity of the system. Includes unexpected traffic that was the result of media-stimulated calling, natural disasters, political or social activities, or other external conditions. If failure was the result of poor event notification and planning or network management response to media-stimulated call-in, or a result of inadequate capacity engineering, consider root cause procedural.

#### **Power Failure**

Instances of outage directly related to failure of the external power system, or failures of service provider back-up power systems. Includes failures associated with commercial power, standby generators, building electrical systems, dc power plants, dc distribution systems, and alarms/monitoring systems. Does not include failures of dc/dc converters or fuses embedded in switches and transmission equipment, unless the problem was caused by the power plant. If the failure was the result of inadequate/no response to (alarmed/un-alarmed) failures, consider root power alarm fault. If the failure was the result of overloaded or undersized power equipment, consider root cause procedural or design fault.

### **Other/Unknown**

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Does not include cases where outage data was insufficient or missing, or where direct cause is still under investigation. When direct cause cannot be proven, it is usually still possible to determine probable cause, which is preferred to the use of "unknown." When classifications provided do not match direct cause, approximate match is preferred to the use of "other."

#### **Insufficient Data**

Failure report (and subsequent investigation, if any) did not provide enough information to determine direct cause of failure.

## **ROOT CAUSE**

### **Procedural - Service Provider**

**Insufficient training**

Training not available from vendor; training not available from service provider; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

**Insufficient staffing**

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resourceintensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

**Insufficient supervision/control**

Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc. This category should be used when multiple procedural causes are reported

**Documentation/procedures unavailable/unclear/incomplete**

Documentation or procedures (vendor or service provider) not published; published, but not distributed; distributed, but not available on-site, etc.

Documentation/procedures obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

**Documentation/procedures out-of-date unusable or impractical**

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation/procedures unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

**Inadequate routine maintenance/memory back-up**

Failure would have been prevented/minimized by simple maintenance routines; recovery action was delayed/complicated by old or missing program/office data tapes or disks, etc.

**Cable unlocated**

Prior notification was provided by the excavator but the facility owner or locating company failed to establish the presence of a cable which was then eventually damaged.

**Inaccurate cable locate**

The cables' presence was determined, but their locations were inaccurately identified.

**Other**

**Procedural - System Vendor**

**Insufficient training**

Training not available from vendor; training not available from service provider; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

**Insufficient staffing**

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or

centralization arrangement; resourceintensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

**Insufficient supervision/control**

Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc. This category should be used when multiple procedural causes are reported

**Documentation/procedures unavailable, unclear, incomplete**

Documentation or procedures (vendor or service provider) not published; published, but not distributed; distributed, but not available on-site.

Documentation obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

**Documentation/procedures out-of-date, unusable, impractical**

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

**Ad hoc activities, outside scope of MOP**

Unapproved, unauthorized work or changes in agreed-to procedures.

**Other**

**Procedural - Other Vendor**

**Insufficient training**

Training not available from vendor; training not available from service provider; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

**Insufficient supervision/control**

Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc. This category should be used when multiple procedural causes are reported

**Documentation/procedures unavailable, incomplete**

Documentation or procedures (vendor or service provider) not published; published, but not distributed; distributed, but not available on-site.

Documentation obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

**Documentation/procedures out-of-date, unusable, impractical**

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

**Ad hoc activities, outside scope of MOP**

Unapproved, unauthorized work or changes in agreed-to procedures.

**Other**

**Design - Software**

**Inadequate defensive checks**

Changes to critical or protected memory were allowed without system challenge; contradictory or ambiguous system input commands were interpreted/responded to without system challenge. Failure of system to recognize or communicate query/warning in response to commands with obvious major system/network impact.

**Ineffective fault recovery or re-initialization action**

Simple, single-point failure resulting in total system outage; failure of system diagnostics that resulted in removal of good unit with restoral of faulty mate; failure to switch/protection switch to standby/spare/mate component(s).

**Faulty software load - program date**

Bad program code/instructions; logical errors/incompatibility between features/sets; software quality control failure; wrong/defective program load supplied.

**Faulty software load - office date**

Inaccurate/mismatched office configuration data used/applied; wrong/defective office load supplied.

**Other**

**Design - Firmware**

**Insufficient software state indications**

Failure to communicate or display out-of-service firmware states; failure to identify, communicate or display indolent or "sleepy" firmware states.

**Ineffective fault recovery or re-initialization action**

Failure to reset/restore following general/system restoral/initialization.

**Other**

**Design - Hardware**

**Inadequate grounding strategy**

Insufficient component grounding design; duplex components/systems sharing common power feeds/fusing.

**Poor backplane or pin arrangement**

Non-standard/confusing pin arrangements or pin numbering schemes; insufficient room or clearance between pins; backplane/pin crowding.

**Poor card/frame mechanisms (latches, slots, jacks, etc.)**

Mechanical/physical design problems.

**Insufficient component/redundancy/diversity**

System design with unnecessary aggregation of components or features; or system deployment with single-point-of-failure configurations.

**Insufficient network redundancy/diversity**

Network design with unnecessary aggregation of systems or network deployment (e.g., CCS network, self-healing rings) with single-point-of-failure configurations.

**Other**

**Hardware Failure**

**Processor community failure**

**Memory unit failure**

## **Peripheral unit failure**

### **Other**

**External Environment** (for limited use when applicable root causes actionable by service provider or vendor cannot be identified)

#### **Lightning/transient voltage**

Component destruction or fault associated with surges and over-voltages caused by (electrical) atmospheric disturbances.

#### **Storm - wind/trees**

Component destruction or fault associated with wind-borne debris or falling trees/limbs.

#### **Storm - water/ice**

Component destruction or fault associated with fog, rain, hail, sleet, snow, or the accumulation of water/ice (flooding, collapse under weight of snow, etc.).

#### **Vehicular accident**

Component destruction or fault associated with motor vehicle (car, truck, train, etc.) collision.

#### **Vandalism/theft**

Component loss, destruction, or fault associated with larceny, mischief, or other malicious acts.

#### **Earthquake**

Component destruction or fault associated directly or indirectly with seismic shock (if damage was the result of inadequate earthquake bracing, consider hardware design fault).

#### **Fire**

Component destruction or fault associated with fire occurring/starting outside service provider plant, includes brush fires, pole fires, etc.

### **Other**

## **Cable Damage**

### **Digging error**

Excavator error during digging (contractor provided accurate notification, route was accurately located and marked, and cable was buried at a proper depth with sufficient clearance from other sub-surface structures).

### **Inadequate/no notification**

Excavator failed to provide any notification prior to digging, or did not accurately describe the location of the digging work to be performed. (Because of the success in avoiding dig-ups by acting upon prior notification, the lack of notification is considered to be the root cause of every dig-up in which prior notification was not provided.)

### **Shallow cable**

The cable was at too shallow a depth, (notification was adequate, locate was accurate, excavator followed standard procedures).

### **Other**

## **Internal Environment**

### **Roof/air conditioning leak**

Component destruction or fault associated with water damage (direct or electrolytic) caused by roof or environmental systems leaks into/in central office environment.

**Manhole/cable vault leak**

Component destruction or fault associated with water entering manholes cable vaults, CEVs, etc.

**Cable pressurization failure**

Component destruction of fault associated with cable damage resulting from cable pressurization failure.

**Environmental system failure (heat/humidity)**

Component loss or fault associated with extreme temperature, rapid temperature changes, or high humidity due to loss/malfunction of environmental control(s). If the failure was the result of inadequate/no response to (alarmed/un-alarmed) environmental failures, or due to incorrect manual control of environmental systems, consider procedural.

**Fire suppression (water, chemicals) damage**

Component loss or fault associated with corrosion (electrolytic or other) caused by fire suppression activities; root cause assumes no substantial failure was directly associated with the smoke/fire that triggered suppression.

**Fire, arcing, smoke damage**

Component loss or fault associated with damage directly related to central office or equipment fires (open flame or smoldering), corrosive smoke emissions, or electrical arcing (whether or not ignition of surrounding material occurs).

**Dirt, dust contamination**

Component loss or fault associated with dirt or dust, typically resulting in component overheating, or loss of connectivity.

**Other**

**Traffic/System Overload**

**Media-stimulated calling - insufficient notification**

System/network overload/congestion directly associated with media-stimulated calling event where event sponsor/generator failed to provide adequate advance notice, or provided inaccurate (underestimated) notification.

**Mass calling - focused/diffuse network overload**

System/network overload/congestion directly associated with unplanned, external trigger(s) causing a significant, unmanageable traffic load.

**Common channel signaling network overload**

CCS system/network overload associated with (true) high traffic loads congesting STP/SCP processors or CCS link network. If overload was associated with STP/SCP message handling congestion, false or reactivated link congestion, inappropriate or incorrect CCS network management message(s), protocol errors, etc., consider software design fault.

**Inappropriate/insufficient NM control(s)**

System/network overload/congestion associated with ineffective NM system/switch response, either because no effective NM control was available, system/switch response to control was inappropriate, or its implementation was

flawed. If failure was related to inappropriate control strategy or execution by NM organization, consider procedural.

**Ineffective engineering/engineering tools**

System/network overload/congestion directly associated with under-engineering of the system/network due to rapidly changing network demand, or introduction of new network components and/or technologies. If failure was associated with simple under-engineering (absent changing environment), consider procedural.

**Other**

**Power Failure** (does not include failures of dc/dc converters or fuses embedded in switches and transmission equipment, which should be reported as a hardware failure, unless the problem was caused by the power plant.)

**Inadequate/missing power alarm**

System failure associated un-alarmed (or under-alarmed) power failure; alarm not provided initially due to inadequate standards or failure to implement standards; alarm/alarm system failure (broken or modified). (Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural.)

**Insufficient response to power alarm**

System failure associated response to power failure: alarm system worked but support personnel did not respond properly. (Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural.)

**Lack of routine maintenance/testing**

System failure that could have been avoided had periodic power system testing, maintenance and/or detailed inspection been performed.

**Overloaded/undersized power equipment**

System failure attributable to insufficient sizing/design of power configuration.

**Lack of power diversification**

Failure to diversify equipment among redundant power system components, including ac rectifiers/chargers, battery power plant, dc distribution facilities, etc.

**Lack of power redundancy**

Failure directly associated with insufficient redundancy of power system components, including ac rectifiers/chargers, battery power plan, dc distribution facilities, etc.

**Inadequate site-specific power contingency plans**

System failure that could have been avoided/minimized had emergency operating procedures and contingency plans been available; outage was prolonged because of lack of site-specific information including equipment engineering data, portable engine hook-up hardware/procedures, load shedding plans, etc.

### **Extended Commercial Power Failure**

System failure due to commercial power failure that extends beyond the design back-up capabilities at the location and beyond reasonable contingency planning assumptions.

#### **Other**

### **Operations Support/Strategy**

#### **Insufficient surveillance capability**

System failure that could have been avoided/minimized had remote operations been able to better "see" system performance; total/comprehensive view of system not available. Surveillance system/links unavailable/out-of-service.

#### **Inadequate control capability**

System failure that could have been avoided/minimized had remote operations been able to better control system performance; comprehensive controls only available on-site. Control system/links unavailable/out-of-service.

#### **Ineffective roll-down or hand-off activity**

System failure that could have been avoided/minimized had better communication and/or process control been in place between/among operations organizations.

#### **Ineffective alarm threshold/display**

System failure that could have been avoided/minimized had user-programmed threshold/display indicators/messages been more effective/explicit.

#### **Impractical trouble-correlation among operations systems**

System failure that could have been avoided/minimized had output of disparate operations systems been better integrated/intelligible - unreasonable output language/naming convention differences among operations systems.

#### **Other**

### **Other/Unknown**

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Does not include cases where outage data was insufficient or missing, or where root cause is still under investigation. When root cause cannot be proven, it is usually still possible to determine probable cause, which is preferred to the use of "unknown." When classifications provided do not match root cause, approximate match is preferred to the use of "other."

### **Insufficient Data**

Failure report (and subsequent investigation, if any) did not provide enough information to determine direct cause of failure.

## **7.6 Sources**

Following are web links to sources referred to in this document

- 47 C.F.R. § 63.100 - <http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr/2003/octqtr/47cfr63.100.htm>
- NRIC - [www.nric.org](http://www.nric.org)
- NRIC Best Practices - <http://www.bell-labs.com/cgi-user/krauscher/bestp.pl>

- NRSC Direct and Root Cause Definitions - <http://www.atis.org/NRSC/Docs/NRSCDefinitions.pdf>
- New Part 4 of the Commission's Rules Concerning Disruptions to Communications, FCC 04-188 [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-04-188A1.doc](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-188A1.doc)

## 8 Appendix 2 - Definitions and Acronyms

### 8.1 *NENA Master Glossary of 9-1-1 Terminology*<sup>13</sup>

See the attached file entitled " FG1C\_Appendix2\_8.1\_ NENA Master Glossary.PDF"

---

<sup>13</sup> [www.nena.org](http://www.nena.org)