



# **Network Outage Reporting System**

***User Manual***

**Version 1**

**November 30, 2004**

# Table of Contents

<b>1</b>	<b>Using the System .....</b>	<b>1</b>
1.1	Accessing the Network Outage Reporting System.....	1
1.2	Security Banner.....	1
1.3	NORS Login .....	2
1.4	Screen for New Users with New Notifications.....	3
1.5	User Menu Screen.....	4
1.6	Notification Screen .....	4
1.7	Screen for Selecting the Report to Modify, File or Withdraw.....	5
1.8	Screen for Modifying and Submitting Initial, Draft and Final Reports .....	6
1.9	Submitting a Final Report.....	7
1.10	Screen to View Notifications, Initial and Final Reports.....	8
<b>2</b>	<b>Fields on the Notification Form .....</b>	<b>9</b>
<b>3</b>	<b>Fields on the Initial and Final Report Forms.....</b>	<b>12</b>
<b>4</b>	<b>Descriptions of Root Cause, Direct Cause and Contributing Factors .....</b>	<b>19</b>

# 1 Using the System

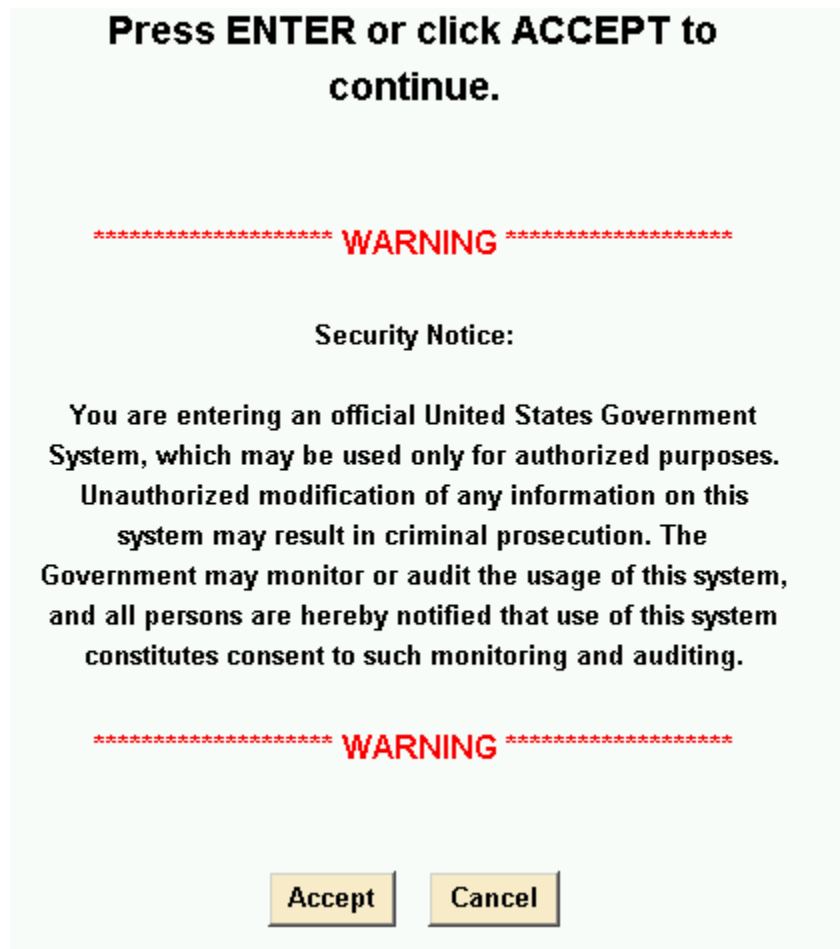
## 1.1 Accessing the Network Outage Reporting System

The Network Outage Reporting System (NORS) can be accessed by first going to the FCC homepage. The address is [www.fcc.gov](http://www.fcc.gov). Once you are at the FCC homepage, you can find the NORS under the E-Filing menu at the top of the page. Alternately you can go to the Engineering & Technology under Offices on the right side of the home page. Finally, you may go directly to the NORS using the following URLs:

<https://svartifoss2.fcc.gov/prod/oet/ntd/outage/NORS.cfm>

## 1.2 Security Banner

The following Security Banner will be displayed once the URL for the NORS has been sent:



You will have to acknowledge that you “accept” the conditions stated in the Security Banner.



### 1.3 NORS Login

You will then indicate whether you are retrieving outage reports or filing outage reports. If you are editing or withdrawing outage reports, you should use the Filing Module. All new users should pick the Filing Module.

Welcome to the home page of the  
**Network Outage Reporting System (NORS)**

*This system is comprised of two separate modules for filing and retrieving outage reports.*

*To continue, choose one of the following:*

<b>Retrieval Module *</b>  <a href="#">Retrieve Outage reports</a>	<b>Filing Module **</b>  <a href="#">Report Network Outage</a>
---	---

\* For Department of Homeland Security.  
\*\* For companies filing, modifying and withdrawing outage reports.

In either case, you will get to a login screen. The Login screen is used to allow outage analysts, outage coordinators and outage inputters to have access to the system. You will need a User ID and a password. The NORS system User ID and password will be authenticated when you click the Login button on the login screen. The login screen for Filing Outages is:

**Network Outage Report System - Filing Login**

UserName:

Password:

If you don't have username/password, please click [here](#)

If you have questions about this web page, please contact [FCC Outage Help](#).

If you do not already have a User ID and Password, you should click the link marked “please click here”. This will send you to the New User screen.

The login screen for Retrieving Outages is:

**Network Outage Report Login**

UserName:

Password:

If you have questions about this web page, please contact [FCC Outage Help](#).

Only users with a valid User ID and Password can log onto the NORS to retrieve outage reports.

#### **1.4 Screen for New Users with New Notifications**

If you do not already have UserID, you will be required to identify yourself including providing a valid e-mail address. The system will respond with your User ID and password. You will then be allowed to file notifications. You will also be able to file and edit initial and final outage reports for the outages for which you have submitted the original notification. The screen for New Users is:

**New User**

Reporting Company:

New Company:

Contact Person:

Phone Number:  (###-###-####) Extension:

E-Mail:

You will then be sent to the following screen which provides your UserID and password. You can then log onto the NORS and notify the FCC of the outage.

## New Reporting Carrier

Your new Username (healyj) and Password (89403301) have been assigned.

DONE

### 1.5 User Menu Screen

Those users with valid User IDs and valid passwords who are filing (editing or withdrawing) an outage will go to the User Menu Screen upon logging on. This screen is shown below:

#### Network Outage Report System - Main Menu

- [Report Notification](#) -- To create new outage report.
- [Modify/Resubmit/Withdraw Report](#) -- To modify/resubmit/withdraw existing outage report.

This screen allows you to submit a notification or to submit an initial or final report. If you choose “Report Notification,” you will be sent to the Notification Screen. If you are notifying the FCC of a new outage, you should choose “Report Notification.” If you want to modify, submit or withdraw an initial or final report, you should choose “Modify/Resubmit/Withdraw Report.”

### 1.6 Notification Screen

To submit a notification, you must fill out the following screen:

## Notification of New Outage Report

**Name of Reporting Entity** (e.g., Company): TEST COMPANY  
**Type of Entity Reporting Disruption:** Cable telephony provider  
**Date of Incident:** 11/09/2004  
**Local Time Incident Began (24 hr clock (nnnn)):**  **Time Zone:** Eastern

**Effects of the Outage**

**Number of Potentially Affected**

**Wireline Users:**   
**Wireless (non-paging) Users:**   
**Paging Users:**   
**Cable Telephony Users:**   
**Satellite Users:**

**Number Affected**

**Blocked Calls:**  **Real-Time:**  **Historic:**   
**DS3s:**   
**Lost SS7 MTP Messages:**  **Real-Time:**  **Historic:**

**Geographic Area Affected**

**State:** MULTI STATES  
**City:**

**Description of Incident**

**Primary Contact Person:**   
**Phone Number:**  **Extension:**   
**E-mail Address:**

Details on how to fill out each field are given in Section 2. You have 30 minutes to fill in the form. No information will be stored unless you hit the “Submit” button. Once you hit this button, a Notification has been filed if you do not get an error message telling you that one of the fields has been filled out incorrectly. Note that the name of your company can not be changed.

When you are ready to submit an Initial or Final report, you will have to logon to the NORS and access the correct Notification. To do this, you will select “Modify/Resubmit/Withdraw a Report.”

### **1.7 Screen for Selecting the Report to Modify, File or Withdraw**

The following screen will come up for users who select Modify/Resubmit/Withdraw a Report. This screen is for anyone updating a Notification to an Initial, Draft or Final

Report or modifying an Initial or Draft Report. Initial and Final Reports are formally filed reports. The system allows users to save Drafts of reports. No government agencies outside the FCC (including DHS) can see Drafts.

### Network Outage Report System - List

From: 11 18 2004 To: 11 18 2004 Report Type: All RETRIEVE

Reference Number	Report Type	Company Name	Initial Filing Date/Time	Updated Date/Time			
04-0002	Notification	TEST COMPANY	11/18/2004 12:24	N/A	DISPLAY	MODIFY	WITHDRAW
04-0001	Initial	TEST COMPANY	11/18/2004 12:23	11/18/2004 12:25	DISPLAY	MODIFY	WITHDRAW

You will be able to list all the outages that you are able to modify, resubmit and withdraw. Outage inputters will be able to modify (and access) only the outages that they personally have already submitted. Outage coordinators will be allowed to modify, resubmit and withdraw any outage except Final reports from their company.

If you select a report except a Final Report, you will be able to modify, resubmit or withdraw it. In particular, if you choose a notification, you will be able to modify it and then submit it as an Initial or Final Report. Any reports that are withdrawn are not deleted from the database – they are marked as withdrawn.

### 1.8 Screen for Modifying and Submitting Initial, Draft and Final Reports

The following screen will come up once you have selected a report to modify and resubmit. The screen will be populated with the most recent version of the report. **This form must be filled out in 30 minutes and submitted.** This means that the text for most of the text fields should be already prepared and cut and pasted into the form. If you do not hit the “Submit” button for 30 minutes, all your changes will be lost and you will have to start over (logon to NORS again)

The top of this form is printed below. In section 3, there is detailed explanation of how to fill out each of the fields.



## Outage Report

Report Number: 04-0059

Initial Filing Date-Time: 11/09/2004 13:51

<a href="#">Report Type:</a>	<input type="text" value="Initial Report"/>	
<a href="#">Name of Reporting Entity (e.g., Company):</a>	TEST COMPANY	
<a href="#">Type of Entity Reporting Disruption:</a>	Cable telephony provider	
<a href="#">Date of Incident:</a>	<input type="text" value="11/09/2004"/>	
<a href="#">Local Time Incident Began (24 hr clock (nnnn)):</a>	<input type="text" value="0900"/>	<a href="#">Time Zone:</a> <input type="text" value="Eastern"/>
<a href="#">Outage Duration:</a>	<input type="text" value="3"/> Hrs	<input type="text" value="0"/> Min
<a href="#">Explanation of Outage Duration (for incidents with partial restoration times)</a>		
<input type="text"/>		
<a href="#">Inside Building:</a>	<input type="text" value="Yes"/>	

### 1.9 Submitting a Final Report

If the report type is a Final Report and you hit the submit button, the following screen will come up:

**Security Notice:**

**I am authorized by the communications provider to legally bind the provider to the truth, completeness, and accuracy of the information contained in this report. I attest that I have read the report prior to submitting it and on oath depose and state that the information contained therein is true, correct, and accurate to the best of my knowledge and belief, and that the communications provider on oath deposes and states that this information is true, complete, and accurate.**

To actually submit the Final Report, you will accept the above statement that states that you are authorized to submit the report and that your company deposes and states that the information is true, complete, and accurate.

### 1.10 Screen to View Notifications, Initial and Final Reports

Outage inputters can not view outages from other companies. The NORS has a module so that DHS can view outages. If you have chosen the retrieval module, have successfully logged onto the NORS (see Section 1.3) and have access to the retrieval module, you may select an outage to view.

**Network Outage Report System - List**

From:   To:

Reference Number	Report Type	Initial Filing Date/Time	Updated Date/Time	
04-0051	Final	10/15/2004 11:50:40	10/18/2004 14:11:33	<input type="button" value="DISPLAY"/>
04-0051	Final	10/15/2004 11:50:40	10/18/2004 13:48:28	<input type="button" value="DISPLAY"/>
04-0051	Initial	10/15/2004 11:50:40	10/18/2004 13:47:32	<input type="button" value="DISPLAY"/>
04-0051	Initial	10/15/2004 11:50:40	10/18/2004 13:44:07	<input type="button" value="DISPLAY"/>
04-0051	Initial	10/15/2004 11:50:40	10/18/2004 13:42:04	<input type="button" value="DISPLAY"/>

## 2 Fields on the Notification Form

**Name of Reporting Entity** – lists the name of the company filing the outage report. This field is automatically filled out. It is the name of the company that the outage inputter used when he/she applied for a UserID. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, E911 service provider, or facility owner that experiences an outage meeting the reporting thresholds as defined in Part 4 of the Commission's Rules and Regulations on any facilities which it owns, operates or leases.

**Type of Entity Reporting Disruption** – pick from the scroll down menu the type entity your company is. The choices are:

- Wireline carrier
- Wireless carrier
- Cable telephony provider
- Paging provider
- Satellite provider
- SS7 network provider
- E911 service provider
- Facility owner or operator

If a company is a carrier like BellSouth which provides SS7 service, E911 service and is a facility owner, that carrier should identify itself as a wireline carrier. The designation SS7 network provider is for companies that only provide SS7 service and are not carriers. Similarly the designation E911 service provider is for companies that only provide some portion of E911 service and are not carriers. The designation facility owner is for companies that are not carriers but own, operate and lease facilities for use in telecommunications.

**Date of Incident** - provide the month, day and year at the commencement of the outage. The expected format is mm/dd/yyyy.

**Local Time Incident Began (24 hr clock)** - provide the local time at the location of the, outage (not the reporting location) of commencement of the outage (24-hour clock). That is, for 1:00 PM, you should use 1300. The format should be nnnn; that is, do not use a colon. Acceptable inputs would be 800, 0800, 2300, etc. This number should be between 0 and 2359. In most cases both the physical location of the outage and the majority of effects of the outage are in the same time zone. However, some outages have wide-ranging impacts and at times the greatest customer impact may not be at the physical location of the outage. For undersea cables cut, provide the time at the closest end of the undersea cable to the US. You should provide detailed explanations in the Initial or Final Report.

**Time Zone** – Pick from the scroll down menu one of the following:

Atlantic  
Eastern  
Central  
Mountain  
Pacific  
Alaskan  
Hawaii-Aleutian  
Guam  
Other

Puerto Rico is in the Atlantic Time zone. Other should be used for some place like American Samoa.

### **Number of Potentially Affected**

**Wireline Users** – provide the sum of the number of assigned telephone numbers potentially affected by the outage and the number of administrative numbers potentially affected. If this outage did not affect wireline users, please leave this blank. Assigned numbers are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use and include DID numbers. This excludes numbers that are not yet working but have a service order pending. “Administrative numbers” are defined as the telephone numbers used by communications providers to perform internal administrative or operational functions necessary to maintain reasonable quality of service standards.

**Wireless Users** – provide the number of potentially affected wireless users. If this outage did not affect wireless users, please leave this blank. In determining the number of users potentially affected by a failure of a switch, a concentration ratio of 8 shall be applied.

**Paging Users** - provide the number of assigned telephone numbers for those paging networks in which each individual user is assigned a telephone number. If this outage did not affect paging users, please leave this blank. Assigned numbers are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use. This excludes numbers that are not yet working but have a service order pending.

**Cable Telephony Users** - provide the number of assigned telephone numbers. If this outage did not affect cable telephony users, please leave this blank. Assigned numbers are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use and include DID numbers. This excludes numbers that are not yet working but have a service order pending.

**Satellite Users** – provide the number of satellite users affected (if known)

**Number of Affected**

**Blocked Calls** – provide the number of blocked calls. If no calls were blocked, please put 0 down. For interoffice facilities which handle traffic in both directions and for which blocked call information is available in one direction only, the total number of blocked calls shall be estimated as twice the number of blocked calls determined for the available direction. Providers may use historic carried call load data for the same day(s) of the week and the same time(s) of day as the outage, and for a time interval not older than 90 days preceding the onset of the outage, to estimate blocked calls whenever it is not possible to obtain real time blocked call counts. In this case, the number of blocked calls reported should be 3 times historic carried load. In situations where, for whatever reason, real-time and historic carried call load data are unavailable to the provider, even after a detailed investigation, the provider must determine the carried call load based on data obtained in the time interval between the repair of the outage and the due date for the final report; this data must cover the same day of the week, the same time of day, and the same duration as the outage. Justification that such data accurately estimates the traffic that would have been carried at the time of the outage had the outage not occurred must be available on request. In this case, the number of blocked calls reported should be 3 times carried load. The number of blocked calls should be filled out even if it is not the trigger for an outage being reportable.

**Real-Time, Historic Check Box** - check off whether the number of blocked calls came from real-time data or was based on historic carried loads the same day(s) of the week and the same time(s) of day as the outage.

**DS3s** – provide the number of previously operating DS3s that were affected by the outage regardless of the services carried on the DS3s or the utilization of the DS3s.

**Lost SS7 MTP Messages** - In cases of an SS7 outage and where an SS7 provider cannot directly estimate the number of blocked calls, provide the number of real-time lost SS7 MTP messages or the number SS7 MTP messages carried on a historical basis. Historic carried SS7 MTP messages shall be for the same day(s) of the week and the same time(s) of day as the outage, and for a time interval not older than 90 days preceding the onset of the outage. If the outage does not affect an SS7 network, please leave this field blank

**Geographic Area Affected**

**State** – choose the (primary) state from the scroll down menu affected by the outage. All 50 states along with the District of Columbia and Puerto Rico are listed. In addition outages affecting major parts of more than one state should be

listed as multi-state. Finally, if an outage occurred outside the fifty states, the District of Columbia, or Puerto Rico, please choose "Outside the 50 States".

**City** – provide the (primary) city affected.

**Description of Incident** - provide a narrative which describes the sequence of events leading up to the incident, steps taken to try and resolve the incident once it had occurred, and the action(s) which finally brought resolution to the incident. Include any factors which may have contributed to the duration of the incident, "quick fix" actions which may have resolved the immediate problem but were not the final, long-term solution, and any other contributing factors which may aid the reader in better understanding the incident. At the notification stage, it is anticipated that many of the details will not be known.

**Primary Contact Person** – provide the full name of the primary contact person

**Phone Number** – provide the phone number of the primary contact person in the format nnn-xxx-nnnn. That is, 201-444-5656 would mean that the area code or NPA is 201, the NNX is 444, the line number is 5656.

**Extension** – provide the extension number, if used, in format nnnn.

**E-mail Address** – provide the e-mail address of the primary contact person.

### **3 Fields on the Initial and Final Report Forms**

**Report Number** – lists the unique identifying number for the report. This field is automatically filled in from the Notification.

**Initial Filing Date-Time** – self-explanatory. This field is automatically filled in based on the notification.

**Report Type** – choose the type of report: Initial, Draft or Final. Initial Reports are due within 3 days of the outage. Final Reports are due within 30 days of the outage from when the outage started. The Initial Report shall contain all pertinent information then available on the outage and shall be submitted in good faith. The Final Report shall contain all pertinent information on the outage, including any information that was not contained in, or that has changed from that provided in, the Initial Report.

**Name of Reporting Entity** – lists the name of the company filing the outage report. This field is automatically filled in. It is the name of the company that the outage inputter used when he/she applied for a UserID. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, E911 service provider, or facility owner that experiences an outage meeting the reporting thresholds as defined in Part 4 of the Commission's Rules and Regulations on any facilities which it owns, operates or leases.

**Type of Entity Reporting Disruption** – lists the type entity your company is. This entry is taken from the Notification. The possible entries were:

- Wireline carrier
- Wireless carrier
- Cable telephony provider
- Paging provider
- Satellite provider
- SS7 network provider
- E911 service provider
- Facility owner or operator

**Date of Incident** - provide the month, day and year at the commencement of the outage. The expected format is mm/dd/yyyy.

**Local Time Incident Began (24 hr clock)** - provide the local time at the location of the, outage (not the reporting location) of commencement of the outage (24-hour clock). That is, for 1:00 PM, you should use 1300. The format should be nnnn; that is, do not use a colon. Acceptable inputs would be 800, 0800, 2300, etc. This number should be between 0 and 2359. In most cases both the physical location of the outage and the majority of effects of the outage are in the same time zone. However, some outages have wide-ranging impacts and at times the greatest customer impact may not be at the physical location of the outage. For undersea cables cut, provide the time at the closest end of the undersea cable to the US. Detailed explanations will be provided in the Initial or Final Report.

**Time Zone** – Pick from the scroll down menu one of the following:

- Atlantic
- Eastern
- Central
- Mountain
- Pacific
- Alaskan
- Hawaii-Aleutian
- Guam
- Other

Puerto Rico is in the Atlantic Time zone. Other should be used for some place like American Samoa.

**Outage Duration** - provide the total elapsed time (hours and minutes) from the commencement of the outage as provided in the preceding data fields until restoration of full service. Full service restoration means restoration of service to all customers

impacted by the outage, not only restoration of the service(s) which may have made the outage reportable to the FCC.

**Explanation of Outage Duration (for incidents with partial restoration times) –**

Describe the stages of restoration if different blocks of users were restored at different times. Often times significant blocks of users may be restored to service prior to full restoration of service. If this is the case, information on the number of users in the block restored to service and the elapsed time to partial restoration should be provided so that an accurate assessment of the outage impact may be made. In addition, it is important to report when some services, e.g., E911, are restored if different than other services.

**Inside Building Indicator** – indicate whether the outage occurred inside a building owned, leased, or otherwise controlled by the reporting entity.

**Effects of the Outage - Services Affected**

**Cable Telephony** – check the box if cable telephony users were affected.

**Wireless (other than paging)** - check the box if wireless users were affected.

**E911** - check the box if E911 service or some aspect of E911 service was affected.

**Paging** - check the box if paging users were affected by the outage.

**Satellite** - check the box if satellite facilities were affected by the outage.

**Signaling (SS7)** - check the box if SS7 service was affected by the outage.

**Wireline** - check the box if wireline users were affected by the outage. This includes whether intraLATA or interLATA service was affected.

**Special Facilities (Airport, Government, etc.)** - check the box if some special facility lost telecommunication service.

**Other (please specify)** – Fill in any other services affected.

**Number of Potentially Affected**

**Wireline Users** – provide the sum of the number of assigned telephone numbers potentially affected by the outage and the number of administrative numbers potentially affected. If this outage did not affect wireline users, please leave this blank. Assigned numbers are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use and include DID numbers. This excludes numbers that are not yet working but have a service order pending. “Administrative numbers” are defined as the telephone numbers used by communications providers to perform internal administrative or operational functions necessary to maintain reasonable quality of service standards.

**Wireless Users** – provide the number of potentially affected wireless users. If this outage did not affect wireless users, please leave this blank. In determining the number of users potentially affected by a failure of a switch, a concentration ratio of 8 shall be applied.



**Paging Users** - provide the number of assigned telephone numbers for those paging networks in which each individual user is assigned a telephone number. If this outage did not affect paging users, please leave this blank. Assigned numbers are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use. This excludes numbers that are not yet working but have a service order pending.

**Cable Telephony Users** - provide the number of assigned telephone numbers. If this outage did not affect cable telephony users, please leave this blank. Assigned numbers are defined as the telephone numbers working in the Public Switched Telephone Network under an agreement such as a contract or tariff at the request of specific end users or customers for their use and include DID numbers and include DID numbers. This excludes numbers that are not yet working but have a service order pending.

**Satellite Users** – provide the number of satellite users affected (if known)

#### **Number of Affected**

**Blocked Calls** – provide the number of blocked calls. If no calls were blocked, please put 0 down. For interoffice facilities which handle traffic in both directions and for which blocked call information is available in one direction only, the total number of blocked calls shall be estimated as twice the number of blocked calls determined for the available direction. Providers may use historic carried call load data for the same day(s) of the week and the same time(s) of day as the outage, and for a time interval not older than 90 days preceding the onset of the outage, to estimate blocked calls whenever it is not possible to obtain real time blocked call counts. In this case, the number of blocked calls reported should be 3 times historic carried load. In situations where, for whatever reason, real-time and historic carried call load data are unavailable to the provider, even after a detailed investigation, the provider must determine the carried call load based on data obtained in the time interval between the repair of the outage and the due date for the final report; this data must cover the same day of the week, the same time of day, and the same duration as the outage. Justification that such data accurately estimates the traffic that would have been carried at the time of the outage had the outage not occurred must be available on request. In this case, the number of blocked calls reported should be 3 times carried load. The number of blocked calls should be filled out even if it is not the trigger for an outage being reportable.

**Real-Time, Historic Check Box** - check off whether the number of blocked calls came from real-time data or was based on historic carried loads the same day(s) of the week and the same time(s) of day as the outage.

**DS3s** – provide the number of previously operating DS3s that were affected by the outage.

**Lost SS7 MTP Messages** - In cases of an SS7 outage and where an SS7 provider cannot directly estimate the number of blocked calls, provide the number of real-time lost SS7 MTP messages or the number SS7 MTP messages carried on a historical basis. Historic carried SS7 MTP messages shall be for the same day(s) of the week and the same time(s) of day as the outage, and for a time interval not older than 90 days preceding the onset of the outage. If the outage does not affect an SS7 network, please leave this field blank

### **Geographic Area Affected**

**State** – choose the (primary) state from the scroll down menu affected by the outage. All 50 states along with the District of Columbia and Puerto Rico are listed. In addition outages affecting major parts of more than one state should be listed as multi-state. Finally, if an outage occurred outside the fifty states, the District of Columbia, or Puerto Rico, please choose “Outside the 50 States”.

**City** – provide the (primary) city affected.

**More Complete Description of Geographical Area of Outage** –provide a more complete description of the geographical area of the outage. In particular, for widespread outages affecting several states, it is important to list the states affected. For outages affecting more than one community, it is important to describe actual communities affected. Include CLLIs if applicable.

**Description of Incident** - provide a narrative which describes the sequence of events leading up to the incident, steps taken to try and resolve the incident once it had occurred, and the action(s) which finally brought resolution to the incident. Include any factors which may have contributed to the duration of the incident, "quick fix" actions which may have resolved the immediate problem but were not the final, long-term solution, and any other contributing factors which may aid the reader in better understanding the incident. The description should be sufficiently detailed to allow the reader, in conjunction with other information provided in the report, to reach the same conclusions as the writer as to the Direct Cause and Root Cause of the incident.

**Description of the Cause(s) of the Outage** – provide a text description of all the causes of the outage. This text should be in the own words of outage inputter and should not necessarily use the words contained in the pull-down menus.

**Direct Cause: The direct cause is the immediate event that results in an outage** – scroll down the menu and pick the direct cause that fits best. The direct cause is the event, action or procedure that triggered the outage. In the Appendix there is a complete description of each of the direct causes. For example, a cable cut improper marking could be the triggering event or direct cause but the real cause or root cause may be lack of diversity.

**Root Cause: The root cause is the underlying reason why the outage occurred.** - scroll down the menu and pick the root cause that fits best. Root Cause is the key problem, which once identified and corrected, would prevent the same or a similar problem from recurring. 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 primary causes - the Root Cause. In the Appendix there is a complete description of each of the root causes. For example, a cable cut improper marking could be the triggering event or direct cause but the real cause or root cause may be lack of diversity.

**Contributing Factors** – scroll down the menu and pick the contributing factors that fit best. Contributing factors are problems or causes that are closely linked to the outage. Often if a contributing factor were addressed, the outage could be prevented or the effect of the outage would have been reduced or eliminated. The form allows two contributing factors.

**Diversity Indicator** – determine whether lack of diversity contributed to or caused the outage. That is, determine whether engineering standards for diversity are being followed. In general, if Best Practices related to diversity are discussed in any of the Best Practice fields or if lack of diversity is listed as a root cause or contributing factor to the outage, then the diversity checkbox must also be checked.

**Malicious Activity** – indicate whether you believe that malicious activity might be involved in the outage. Malicious activity could be product of terrorists. If there is malicious activity, the form asks for some explanation of why you believe the activity is malicious or what is suspicious about the activity.

**Name and Type of Equipment that Failed** - provide the vendor name and the specific equipment (including software release if applicable) involved in the outage. For example, if a relay in a power plant fails that subsequently causes a switch to go out of service due to lack of power, report the make and model of the relay, not the switch.

**Specific Part of the Network Involved** – provide the part of the network involved. Examples are local switch, tandem switch, signaling network, central office power plant, digital cross-connect system, outside plant cable, ALI database, etc.

**Method(s) Used to Restore Service** - provide a complete, chronological narrative of the methods used to restore service, both "quick fix" and final.

**Telecommunications Service Priority (TSP) Indicator** – indicate whether TSP was used during service restoration.

**Steps Taken to Prevent Reoccurrence** – provide the steps already taken and to be taken to prevent reoccurrence. These steps could be at both this location and throughout the network(s) if appropriate. Typically the corrective actions are identified through a Root Cause Analysis of the incident. If a time frame for implementation exists it should be

provided. If no further action is required or planned, the service provider should so indicate.

**Applicable Best Practices that might have prevented the Outage or reduced its effects** – provide a description of Best Practices that could have prevented the outage or reduced its effects. The Network Reliability and Interoperability Council has developed a list of Best Practices. They can be accessed via [www.nric.org](http://www.nric.org). You can find relevant Best Practices by using keywords.

**Best Practices used to mitigate effects of Outage** - provide a description of most important Best Practices that were actually used to mitigate the effects of the outage. These Best practices helped shorten the outage, reduced the restoration times, prevented the outage from affecting more customers, or reduced the effects on customers (ensured that E911 was not affected). If none were used, please leave blank.

**Analysis of Best Practices** – provide an evaluation of the relevance, applicability and usefulness of the current Best Practices for the outage. If a new Best Practice is needed or an existing Best Practice needs to be modified, please indicate this.

**Remarks** – provide any additional information that you believe is relevant that did not fit anywhere else on the form.

**Primary Contact Person** – provide the full name of the primary contact person

**Phone Number** – provide the phone number of the primary contact person in the format nnn-xxx-nnnn. That is, 201-444-5656 would mean that the area code or NPA is 201, the NNX is 444, the line number is 5656.

**Extension** – provide the extension number, if used, in format nnnn.

**U.S. Postal Service Address** – provide the address of the primary contact person.

**E-mail Address** – provide the e-mail address of the primary contact person.

**Secondary Contact Person** – provide the full name of the secondary contact person.

**Phone Number** – provide the phone number of the secondary contact person in the format nnn-xxx-nnnn. That is, 201-444-5656 would mean that the area code or NPA is 201, the NNX is 444, the line number is 5656.

**Extension** – provide the extension number, if used, in format nnnn.

**U.S. Postal Service Address** – provide the address of the secondary contact person.

**E-mail Address** – provide the e-mail address of the secondary contact person.

## 4 Descriptions of Root Cause, Direct Cause and Contributing Factors

### Cable Damage

#### **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. This is considered a procedural error.

#### **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.)

#### **Inaccurate cable locate**

The cable's presence was determined, but their locations were inaccurately identified. This is considered a procedural error.

#### **Shallow cable**

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

#### **Other**

### Design - Firmware

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

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

#### **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.

#### **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.

#### **Other**

### Design – Software

#### **Faulty software load - office data**

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

#### **Faulty software load - program data**

Bad program code/instructions; logical errors/incompatibility between features/sets;

software quality control failure; wrong/defective program load supplied.

**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).

**Other**

**Diversity Failure**

**External**

Failure to provide or maintain diversity of links among external network components resulting in a single-point-of-failure configuration.

**Links**

Communication paths not physically and logically diverse.

**Power**

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

**Timing Equipment**

Failure to diversify critical equipment across timing supplies (e.g., BITS clocks)

**Internal (Other)**

Failure to provide or maintain diversity of equipment internal to a building excluding power equipment and timing equipment.

**Environment – External** (for limited use when applicable root causes actionable by service provider or vendor cannot be identified; can be listed as contributing factor)

**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.

**Lightning/transient voltage**

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

**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.).

**Storm - wind/trees**

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

**Vandalism/theft**

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

**Vehicular accident**

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

collision.

**Other**

**Environment (Internal)**

**Cable pressurization failure**

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

**Dirt, dust contamination**

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

**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, 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).

**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.

**Manhole/cable vault leak**

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

**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.

**Other**

**Hardware Failure**

**Memory unit failure**

**Peripheral unit failure**

**Processor community failure**

**Other**

**Insufficient Data**

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

**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."

**Power Failure (Commercial and/or Back-up)** (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.)

**Battery Failure**

Batteries did not function as designed.

**Extended Commercial Power Failure**

System failure due to commercial power failure that extends beyond the design back-up capabilities

**Generator Failure**

Generator did not function as designed or ran out of fuel.

**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.)

**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.

**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 power redundancy**

Failure directly associated with insufficient redundancy of power system components, including ac rectifierschargers, battery power plan, dc distribution facilities, etc

**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

**Other**

**Procedural - Other Vendor**

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

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

**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.

**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.



**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 indicated

**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.

**Other**

**Procedural - Service Provider**

**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.

**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.

**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.

**Insufficient staffing**

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (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 indicated.

**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.

**Other**

**Procedural - System Vendor**

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

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

**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.

**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.

**Insufficient staffing**

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

**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.

**Other**

**Simplex Condition**

**Non-service affecting**

Failure of one side of a duplexed system such as a SONET ring where unprotected simplex service was still provided for the duration of the outage. Do not use this root cause for the complete failure of a duplexed system.

**Service affecting**

Failure of one side of a duplexed system such as a SONET ring where unprotected simplex service was provided for a period of time but was not repaired during the usual maintenance window.

**Traffic/System Overload**

**Common channel signaling network overload**

SS7 system/network overload associated with (true) high traffic loads congesting STP/SCP processors or SS7 link network. If overload was associated with STP/SCP message handling congestion, false or reactivated link congestion, inappropriate or incorrect SS7 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.

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

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

**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.

**Other**