



1200 G Street, NW
Suite 500
Washington, DC 20005

P: 202-628-6380
F: 202-393-5453
W: www.atis.org

ATIS Board Officers

Chair
Kristin Rinne
AT&T

First Vice Chair
Nick Adamo
Cisco Systems

Second Vice Chair
Thomas Sawanobori
Verizon

Treasurer
Joseph Hanley
Telephone and Data
Systems

President & Chief
Executive Officer
Susan M. Miller
ATIS

Vice President of
Finance & Operations
William J. Klein
ATIS

July 19, 2012

Via Email

Jeffrey Goldthorp
Chief, Communications Systems Analysis Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: NRSC Recommendations to the NORS User Manual, Help File,
and Cause Codes

Dear Jeff:

On behalf of its Network Reliability Steering Committee (NRSC), the Alliance for Telecommunications Industry Solutions (ATIS) is writing to provide recommendations for changes to the Network Outage Reporting System (NORS) User Manual Version 6 and NORS Help File. These recommendations, enclosed herewith, are intended to ensure that the content of the User Manual and Help File accurately reflect what is in the production system of NORS.

Additionally, to accommodate VoIP services, modifications were identified for two specific areas of the Cause Codes. This feedback is attached to this letter.

The NRSC appreciates the opportunity to provide these recommendations. If there are any questions regarding this matter, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas Goode", written in a cursive style.

Thomas Goode
ATIS General Counsel

cc: John Healy, Associate Division Chief, Cybersecurity and Communications
Reliability Division

Attachments



Network Outage Reporting System

User Manual

Version 6

April 9, 2009

Table of Contents

1	Logging Onto the Network Outage Reporting System	1
1.1	Accessing the Network Outage Reporting System	1
1.2	Security Banner	1
1.3	NORS Login Screen	2
1.3.1	Screen for New Users with New Notifications	4
1.3.2	Screen for Password Request	5
1.3.3	Password Expiration	6
2	User Main Menu Screen	6
2.1	Find a Report	8
2.2	Report Notification	8
2.3	Update/Resubmit/Withdraw a Report	10
2.3.1	Screen for Updating Notifications, Initial Reports and Drafts, and Filing Final Reports	11
2.3.2	Filing a Final Report	12 12
2.3.3	Withdrawing a Report	12
2.4	Upload XML File	13
2.5	Request to Reopen a Report	13
2.6	Reports Overdue	13
2.7	Report List	14
2.8	Modify Password	15
2.9	Modify Profile	16
2.10	Modify Company ID	16
2.11	Deactivate User	17
2.12	User List	17
2.13	XML Filing Utility	17
2.13.1	Creating XML Facility	19
2.13.2	Creating XML Files	19
3	Screen for DHS (Retrieve Outage Reports)	19
4	Fields on the Notification Form	19
5	Fields on the Initial, Draft, and Final Report Forms	24
6	Fields on the Withdrawn Report Form	32 32
7	Descriptions of Root Cause, Direct Cause and Contributing Factors ...	33 33

1 Logging Onto the Network Outage Reporting System

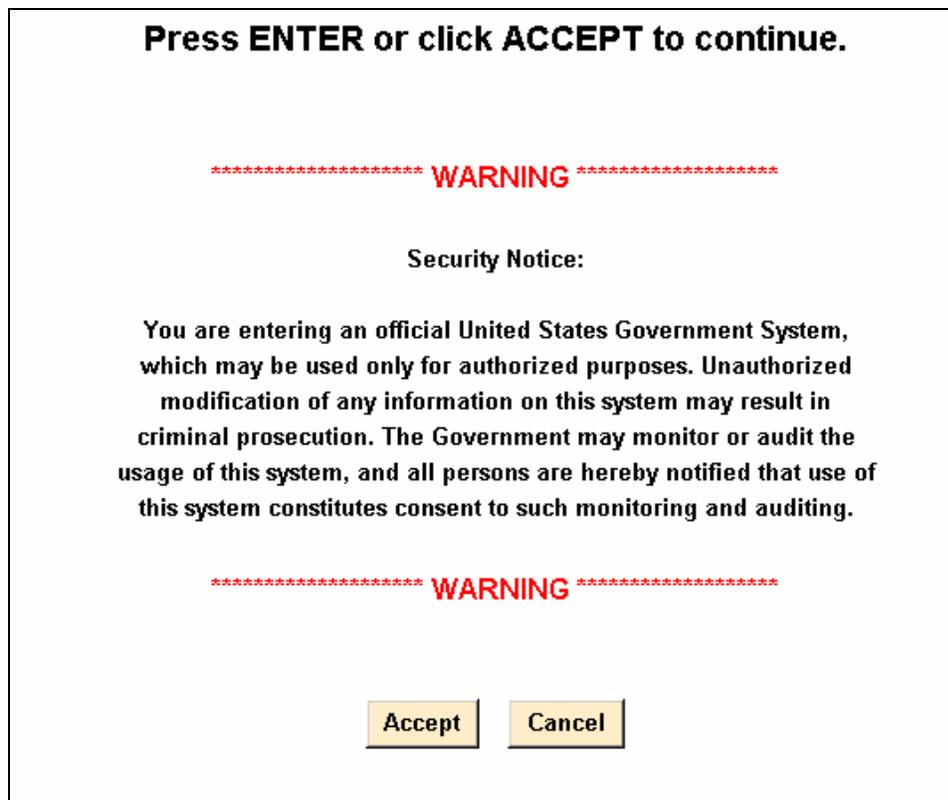
1.1 Accessing the Network Outage Reporting System

The Network Outage Reporting System (NORS) can be accessed by first going to the FCC homepage. The address is www.fcc.gov. Once you are at the FCC homepage, you can find the NORS under the E-Filing menu at the top of the page. Alternatively, you may go directly to NORS using the following URL:

<https://www.fcc.gov/nors/outage/>

1.2 Security Banner

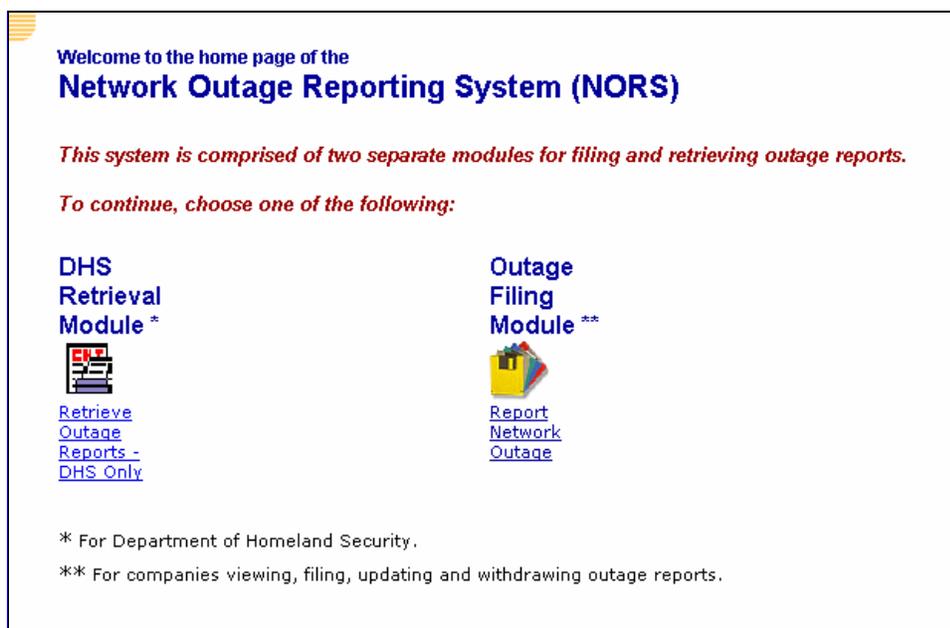
The following Security Banner will be displayed once the URL for the NORS has been sent:



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

1.3 NORS Login Screen

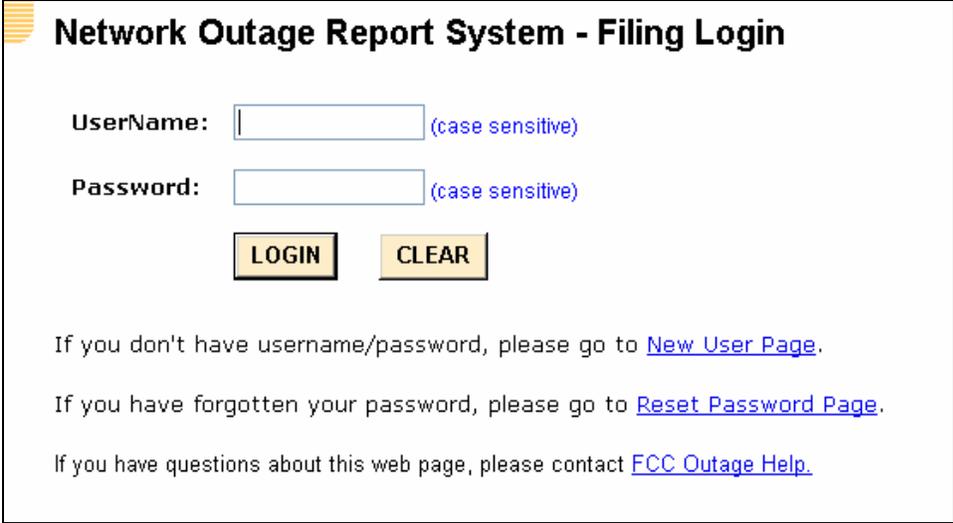
There are two main types of users: Department of Homeland Security (DHS) and all others. DHS will be using the “DHS Retrieval Module.” All others will be using the “Outage [Report Filing and Review](#) Module.” From the Outage [Report Filing and Review](#) Module, you can view, input, update and withdraw outage reports. All new users should pick the Outage [Report Filing and Review](#) Module. In summary, if you are not from DHS, you will use the Outage [Report Filing and Review](#) Module.



Comment [RG1]: Recommend updating system and screen shot from “Outage Filing Module**” to “Outage Report Filing and Review Module**”.

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. The outage inputters can only report Notifications and update/resubmit/withdraw (and access) the outages that they personally have already submitted. An outage coordinator will be allowed to modify, resubmit and withdraw any outage report from his or her company, except for a Final or Withdrawn Report.

The outage coordinator has access to all other inputter reports of their company and can also function as an inputter. You will need a UserID and a password. The NORS system UserID and password will be authenticated when you click the Login button on the Login screen. The Login screen for the Outage [Report Filing and Review](#) Module is:



Network Outage Report System - Filing Login

UserName: (case sensitive)

Password: (case sensitive)

LOGIN **CLEAR**

If you don't have username/password, please go to [New User Page](#).

If you have forgotten your password, please go to [Reset Password Page](#).

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

If you do not already have a UserID and Password, you should click the link marked “If you don’t have username/password, please go to **New User Page**.” This will send you to the New User screen (*see* Section 1.3.1). NOTE: If you forget your password, you should click the link marked, “If you have forgotten your password, please go to **Reset Password Page**.” The system will send you to a screen that asks for your UserID and e-mail address. Your password will be e-mailed to you. If you need help or have questions, click the link marked “If you have questions about this web page, please contact **FCC Outage Help**.”

Formatted: Font: Bold, Font color: Auto

Formatted: No underline, Font color: Auto

Formatted: Font: Bold, Font color: Auto

Formatted: Font: Bold, Font color: Auto

The login screen for DHS to use for Retrieving Outages is:



Network Outage Report Login

UserName: (case sensitive)

Password: (case sensitive)

LOGIN **CLEAR**

If you have forgotten your password, please go to [Reset Password Page](#).

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

Only DHS users with a valid UserID and Password can log onto NORS to retrieve outage reports.

If you are a member of DHS and do not already have a UserID and Password or need help, contact the FCC to obtain a UserID and Password (send an e-mail to FCC-Outage@fcc.gov). If you have forgotten your password, you should click the link marked, “If you have forgotten your password, please go to [Reset Password Page](#).” If you need other help or have other questions, you should click the link marked “If you have questions about this web page, please contact [FCC Outage Help](#).”

Formatted: Font: Bold, Font color: Auto

Formatted: Font: Bold, Font color: Auto

1.3.1 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 UserID and password. You will then be allowed to file Notifications. If you are an inputter, you will also be able to file and edit Initial and Final Reports for the outages for which you have submitted the original Notification. If you are a coordinator, you will be able to file and edit Initial and Final Reports for the outages for which your company has submitted the original Notification. The screen for New Users is:

New User

Notice: Company ID is needed for users from companies on this list (the default is 11111111). Outage Coordinators set this ID for their company. If your are entering a new company name, you may leave the Company ID blank.

Reporting Company: 360NETWORKS (USA), INC.

New Company (Type in new company name if applicable):

Company ID:

Contact Person:

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

E-Mail:

Address:

If your company has filed an outage report or has an outage coordinator, your company will be listed in the scroll down menu under the Reporting Company. You will have to choose that company and know the Company ID (or password). The Company ID is controlled by the outage coordinators for your company (if your company has outage coordinator(s)). The default value for it is 11111111. The Company ID is used to prevent unauthorized access to your company’s outage data on NORS. If your company

is not in the scroll down menu, please give the name of your company. You will not have to provide a Company ID in this case.

In all cases, you must provide your name, phone number and e-mail address. 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

Large companies with many outage inputters may elect to have one or more of the outage inputters converted to outage coordinators. Outage coordinators have the ability to view and update any outage report from their company. Only the NORS administrators can convert an outage inputter to an outage coordinator. If you would like one or more of your outage inputters converted to outage coordinators, send an e-mail to FCC-Outage@fcc.gov. You will then be called and your request processed.

1.3.2 Screen for Password Request

The following Password Request screen appears after someone at the Login screen clicks the link marked “If you have forgotten your password, please go to [Reset Password Page](#).”

Formatted: Font: Bold, Font color: Auto

Network Outage Report System - Password Request

UserName:

E-Mail:

* Email address must be same as the one in the system.

REQUEST

CLEAR

NORS will send you your new password via e-mail.

1.3.3 Password Expiration

NORS keeps track of the time that a password has been operative. After 60 days, when a user logs into NORS, NORS creates a new password, tells the user that a new password has been created and sends the new password to the user's e-mail address. The user can use this new password or can modify the password through the **Modify Password** menu option on the main menu. If the new password is not received at the user's e-mail address, the user can click on **Reset Password Page** on the Login Screen and NORS will send a new password.

Formatted: Font: Bold, Font color: Auto

2 User Main Menu Screen

Those users with valid UserIDs and valid passwords who are filing (editing or withdrawing) an outage will go to the User Main Menu Screen upon logging on. Outage inputters and coordinators have slightly different menus. NORS will authenticate your UserID and password and will send you to the correct user menu.

The Main Menu for coordinators is shown below. The menu for inputters is a subset of the menu for coordinators. The **Request to Reopen a Report** selection, the **List of Open Reports** selection, the **Modify Company ID** selection, the **Deactivate User** selection, the **User List** selection, and the **XML Filing Facility** selection on the menu are available only to outage coordinators. All of the other selections are available to inputters, as well.

Formatted: Font: Bold, Underline, Font color: Auto

Network Outage Report System - Main Menu

- **Find a Report** -- To find a report by report number.
- **Report Notification** -- To create new outage report.
- **Update/Resubmit/Withdraw Report** -- To update/resubmit/withdraw existing outage report.
- **Upload XML File** -- To upload an outage report in XML
- **Request to Reopen a Report** -- To request to reopen Final or Withdrawn Reports.
- **Reports Overdue** -- To get the list of overdue reports.
- **Report List** -- To get the list of reports by selected dates.
- **List of Open Reports** -- To get the list of open reports.
- **Modify Password** -- To modify the password.
- **Modify Profile** -- To modify the user profile.
- **Modify Company ID** -- To modify the company id.
- **Deactivate User** -- To deactivate user.
- **User List** -- To list users.
- **XML Filing Utility** -- To download XML filing utility.

This screen provides a menu of items for managing and handling outage reports. It allows an authorized person to find a report by report number, to notify the FCC of a new outage (Notification), or to update, or withdraw a Notification or Initial Report, or to file a Final Report. Authorized users can request that a Final Report be reopened and obtain a list of reports for which the Finals are overdue or due within 5 days. The last two options, which are only available to outage coordinators, allow them to modify or change the Company ID or to deactivate a user.

If you select **Find a Report**, you will be sent to the “Find a Report” screen to insert the identification number of the particular report you want to retrieve. If you are an outage inputter, this allows you to retrieve a report (by report number) that you have personally submitted. If you are an outage coordinator, you can see a report that you or anyone else from your company has submitted. Note that no one from another company can see reports from your company. The only people allowed to view your outage reports are authorized FCC and DHS personnel, except DHS chooses to release them subject to the terms of our Part 4 Order.¹

If you are notifying the FCC of a new outage, you should choose **Report Notification**. You will be sent to the Notification Screen. If you want to update or withdraw an Initial Report, you should choose **Update/Resubmit/Withdraw Report**. In addition if you want to view your reports, please choose the **Update/Resubmit/Withdraw Report** menu option.

You could also submit the file using **Upload XML File** selection. By providing a XML file name in your computer, it will upload the file to NORS according to the information in the XML file.

NORS has a provision for the user to ask the FCC to reopen a Final or Withdrawn Report by clicking the link marked **Request to Reopen a Report**.

NORS provides a list of Final Reports that are overdue or due within 5 days in order to encourage the timely filing of reports. This function is available by selecting the **Reports Overdue** function on the menu.

NORS can print out a list of outages in spreadsheet format for a set of dates (based on the date the notification was filed). All the information on each outage is provided. To choose this option, select **Report List**.

NORS can print a list of all outage reports that have neither been finalized nor withdrawn. To choose this option, select **List of Open Reports**.

All users should change their password periodically to enhance security of their reporting and viewing of their reports. The menu to change a password is available by selecting **Modify Password**.

Modify Profile allows you to change information in your profile: –your name, phone number, email address and/or address.

The Company ID is a company password maintained by the company’s outage coordinators. It is NORS’ way of allowing companies with outage coordinators to control who can submit outage reports from their company. Anyone who wants to submit outage reports for a particular company must know the Company ID in order to get a UserID that is assigned to that company. Outage coordinators maintain the

¹ Part 4 Report and Order, 19 FCC Red at 16856 ¶ 47.

Company ID. Outage coordinators can change the Company ID. This is done under the heading, **Modify Company ID**.

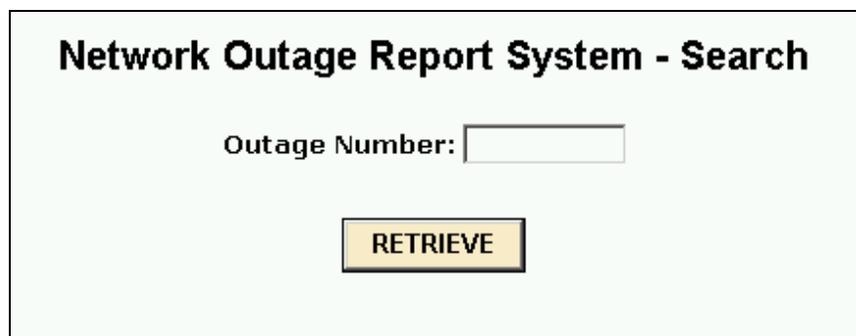
Outage coordinators are allowed to deactivate the privileges of any outage inputters from their company. One coordinator can deactivate another coordinator from their company. This is achieved by selecting **Deactivate User**.

An outage coordinator can print a list of all inputters and coordinators from his or her company. To choose this option, select **User List**.

XML Filing Utility is used to download the utility to help filers to locally create/modify XML files.

2.1 Find a Report

You can review your company's submitted reports by report number. Coordinators have access to all reports filed by their company. Inputters can only see reports that they have filed. NORS will display the following screen after selecting **Find a Report**.



Network Outage Report System - Search

Outage Number:

RETRIEVE

The requested report will be displayed.

2.2 Report Notification

To submit a Notification, you must provide the information on the following screen:

Notification of New Outage Report

If this outage is a national security concern, please call DHS at (703) 235-5080

Name of Reporting Entity (e.g., Company):	TELCO
Type of Entity Reporting Disruption:	<input type="text"/>
Date of Incident:	03/04/2009
Local Time Incident Began (24 hr clock (nnnn)):	<input type="text"/> Time Zone: <input type="text"/>
Reason Reportable:	<input type="text"/>
E911 Outage - Location Affects:	<input type="text"/>
Failure Occurred in Another Companies Network:	<input type="checkbox"/>
Effects of the Outage	
Number of Potentially Affected	
Wireline Users:	<input type="text"/>
Wireless (non-paging) Users:	<input type="text"/>
Paging Users:	<input type="text"/>
Cable Telephony Users:	<input type="text"/>
Satellite Users:	<input type="text"/>
Number Affected	
Blocked Calls:	<input type="text"/> Real-Time: <input type="checkbox"/> Historic: <input type="checkbox"/>
DS3s:	<input type="text"/>
Lost SS7 MTP Messages:	<input type="text"/> Real-Time: <input type="checkbox"/> Historic: <input type="checkbox"/>
Geographic Area Affected	
State, Territory, Commonwealth, or the District of Columbia:	<input type="text"/>
City:	<input type="text"/>
Description of Incident	
<input type="text"/>	
Primary Contact Person:	John Healy
Phone Number:	202-418-2448 Extension: <input type="text"/>
E-mail Address:	john.healy@fcc.gov

Details on how to fill out each field are given in Section 4. Any values provided in one or more of the numeric fields are considered to be the "best guess" at this point in time. All values can be changed in the subsequent Initial and/or Final Reports. You have 60 minutes to fill in the form. The timer shows in the status bar at the bottom left of the screen. *No information will be stored unless you hit the "Submit" button.* Once you hit this button, the Notification has been filed unless an error message appears telling you that one or more of the fields has been filled out incorrectly. You can correct the data and resubmit. NORS will provide the report number for future reference after a successful filing. Note that the name of your company can not be changed. A copy of the completed Notification can be saved in Excel; it can be pasted into an Excel, Word, or text file; or it can be printed using the File>Print commands.

When you are ready to submit an Initial or file a Final Report, you must log_{on}-to NORS and access the correct Notification. To do this, select **Update/Resubmit/Withdraw a Report.**

2.3 Update/Resubmit/Withdraw a Report

The system allows you to list reports and then select the report that you want to update (and resubmit) or withdraw. There are five types of reports: Notifications, Initial Reports, Final Reports, Withdrawn Reports and Drafts. A Draft is an informal copy of a report that the system keeps.

The system allows you to choose outages listed by date and by report type. For example, you can list only your Notifications during the month of September. Select “All” to list all report types. NORS also lets you list all “Active” reports – these are reports that are updatable. This includes Notifications, Initial Reports, and Draft Reports, but excludes Finals and Withdrawn Reports.

If you select any updatable report, you will be able to update, and resubmit or withdraw it. In particular, if you choose a Notification, you will be able to modify it and then submit it only as an Initial, Final, or Withdrawn Report. Withdrawn Reports are not deleted from the database – they are simply marked as withdrawn.

The following screen will come up for users who select Update/Resubmit/Withdraw a Report. This screen is for anyone updating a Notification or an Initial or Draft Report. The system allows users to save Drafts of reports and to revise Initial Reports, but not Final Reports.

Network Outage Report System - List											
From:		7	30	2008	To:		8	20	2008	Report Type:	All
Sort By:		Reference Number							RETRIEVE		
Ref. Number	Type	Company	Incident Date	Notification	Updated						
08-21352170	Initial	TESTCO	07/31/2008 10:00	07/31/2008 14:29	07/31/2008 14:37	DISPLAY	UPDATE	WITHDRAW			
08-21351710	Initial	TESTCO	07/31/2008 10:00	07/31/2008 14:21	07/31/2008 14:23	DISPLAY	UPDATE	WITHDRAW			
08-21339451	Final	TESTCO	07/31/2008 08:00	07/31/2008 10:57	07/31/2008 10:59	DISPLAY					
08-21339293	Final	TESTCO	07/31/2008 08:00	07/31/2008 10:54	07/31/2008 14:15	DISPLAY					
08-21252029	Initial	TESTCO	01/03/2007 07:00	07/30/2008 14:27	07/30/2008 14:38	DISPLAY	UPDATE	WITHDRAW			
08-21227844	Notification	TESTCO	07/30/2008 07:00	07/30/2008 07:44	N/A	DISPLAY	UPDATE	WITHDRAW			

No government agencies outside the FCC (including DHS) can see Drafts.

You will be able to create a list of all the outages that you are able to view, update, or withdraw. Outage inputters will be allowed to view, update or withdraw any Notifications, Drafts or Initial reports that they personally have submitted. Outage coordinators can view, update or withdraw any Notifications, Drafts or Initial Reports from their company. No one can update a Final or Withdrawn Report without first reopening it. ~~Users may request the FCC to reopen a Final Report or a Withdrawn Report.~~ Users can request the FCC to reopen a Final Report or a Withdrawn Report, which the FCC can change to “Initial” status. [The option to reopen a Final Report can be found on the NORS User Main Menu screen. To reopen a Withdrawn Report, an email must be sent to the FCC \(FCC-Outage@fcc.gov\).](#)

2.3.1 Screen for Updating Notifications, Initial Reports and Drafts, and Filing Final Reports

The following screen will come up once you have selected a report to update. The screen will present the most recent version of the report. **This form must be filled out in 60 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 within 60 minutes, all your changes will be lost and you will have to start over (logon to NORS again).** The system gives a 10 minute warning. If you still need more time, you may save the file in NORS as a “Draft” and then reopen the draft.

The top of this form is shown below. In section 4, there is a detailed explanation of how to fill out each of the fields.

Outage Report

Report Number: 08-20750739

Updated Date-Time: 07/25/2008 14:25

Report Type: Initial Report

Name of Reporting Entity (e.g., Company): TESTCO

Type of Entity Reporting Disruption: E911 service provider

Date of Incident: 07/25/2008

Local Time Incident Began (24 hr clock (nnnn)): 0800 **Time Zone:** Atlantic

Reason Reportable: Wireline - 900,000 user-minutes

Outage Duration: 0 Hrs 0 Min

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

Inside Building: [Dropdown]

E911 Outage - Location Affects: [Dropdown]

Comment [RG2]: Insert new screen shot reflecting discovery/date/time fields.

2.3.2 Filing 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 file the Final Report, you must accept the above statement that states that you are authorized by your company to file the Final Report to the Commission; that you are authorized by your company to legally bind it to the truth, completeness, and accuracy of the information contained in the Final Report; and that you attest that you have read the Final Report and depose and state under oath that the information therein is true, correct, and accurate to the best of your knowledge and belief and the company that you represent under oath deposes and states that the information is true, complete, and accurate.

2.3.3 Withdrawing a Report

Occasionally, after filing a **N**otification and perhaps an **I**nitial **R**eport, you may subsequently determine that the outage did not meet the reporting criteria. Such a report should be withdrawn. To withdraw a report, you need to select the report that you want to withdraw from the list of outage reports. When you do, you will see the information contained in the outage report and be presented with a text box, which asks for the reason for withdrawing the report.

Withdrawn **R**eports should be internally consistent. For example, if the reason for Withdrawal is that the outage duration was less than thirty minutes, then the outage duration shown in the report should be less than thirty minutes, etc. When withdrawing a report, the only field changes that are allowed to be made are the primary contact, the secondary contact, and the reason for withdrawing the report. Therefore, changes to any

other fields should be made before changing the report's status to "Withdrawn." That is, if the values shown in the Notification are incorrect, it may be necessary first to update the Notification to an Initial [R](#)report with the correct values before withdrawing it.

2.4 Upload XML File

This screen allows you to submit outage reports in XML format. There is a utility provided to help you prepare XML files (*see* Section [4.182.13](#)). Once you provide the name of the XML file, it will be uploaded to NORS according to the information in the file.

Upload Outage Report in XML

2.5 Request to Reopen a Report

This screen allows outage coordinators to request to reopen ~~either~~ a Final ~~or Withdrawn~~ [R](#)report. Recall that Final [R](#)reports and Withdrawn [R](#)reports cannot be updated. The request is then forwarded to the FCC which then changes the report to an Initial [R](#)report, which can be updated. You need to provide both Company ID and Report Number to request to reopen a report.

Network Outage Report System - Request to Reopen Final or Withdrawn Report

Company ID:

Report Number:

Comment [RG3]: Update screen shot-current does not mention Withdrawn Reports.

2.6 Reports Overdue

NORS provides information on reports that are overdue and reports that will be due in 5 days. To get a listing of these reports, select **Reports Overdue** from the Main Menu. The result of such a query is shown below:

Overdue Reports As of 08/20/2008

Overdue Initial Reports

Reference Number	Company	Notification Date - Time	POC	Phone Number	Email
07-03735436	TESTCO	02/06/2007 - 0900	David Ahn	202-418-0853	david.ahn@fcc.gov
07-06729220	TESTCO	03/08/2007 - 0700	John Smith	111-222-3333	testemail@test.com
07-06730948	TESTCO	03/08/2007 - 0700	John Smith	111-222-3333	testemail@test.com
07-07129396	TESTCO	03/12/2007 - 0800	David Ahn	202-418-0853	david.ahn@fcc.gov
07-09932203	TESTCO	04/09/2007 - 0700	John Smith	111-222-3333	testemail@test.com
08-21227844	TESTCO	07/30/2008 - 0700	David Ahn	202-418-0853	david.ahn@fcc.gov

Overdue Final Reports

Reference Number	Company	Notification Date - Time	POC	Phone Number	Email
07-03735436	TESTCO	02/06/2007 - 0900	David Ahn	202-418-0853	david.ahn@fcc.gov
07-06729220	TESTCO	03/08/2007 - 0700	John Smith	111-222-3333	testemail@test.com
07-06730948	TESTCO	03/08/2007 - 0700	John Smith	111-222-3333	testemail@test.com
07-06849167	TESTCO	03/09/2007 - 1200	David Ahn	202-418-0853	david.ahn@fcc.gov
07-07129396	TESTCO	03/12/2007 - 0800	David Ahn	202-418-0853	david.ahn@fcc.gov
07-07133810	TESTCO	03/12/2007 - 0800	David Ahn	202-418-0853	david.ahn@fcc.gov
07-07134313	TESTCO	03/12/2007 - 0800	David Ahn	202-418-0853	david.ahn@fcc.gov
07-07147123	TESTCO	03/12/2007 - 1000	David Ahn	202-418-0853	david.ahn@fcc.gov
07-07336039	TESTCO	03/14/2007 - 0900	David Ahn	202-418-0853	david.ahn@fcc.gov
07-09932203	TESTCO	04/09/2007 - 0700	John Smith	111-222-3333	testemail@test.com
07-10142270	TESTCO	04/11/2007 - 0800	Location: \$ut#%0#%0a	202-418-2448	Location: \$ut#%0#%0a

Final Reports Due Within 5-Days

Reference Number	Company	Notification Date - Time	POC	Phone Number	Email
08-20750739	TESTCO	07/25/2008 - 0800	John Healy	202-418-2448	john.healy@fcc.gov

SAVE AS EXCEL

2.7 Report List

NORS can print out a list of outages in a spreadsheet format for a set of dates (based on the date the notification was filed). When you choose this option, the following screen will appear:

Network Outage Report System - List

From: 8 / 20 / 2008
To: 8 / 20 / 2008
Order: Reference Number

Columns:

- All
- Notification Date
- Updated Date
- Type
- Company
- Entity Type
- Incident Date/Time
- Time Zone
- Duration Hrs
- Duration Min

All the information on each outage can be provided if desired. Alternatively, you may select to show only certain information by holding down the Control Key while you select the individual columns that you want displayed.

You can order the outages by Reference Number (ID Number), type (Notification, Initial Report, etc), incident date, notification date, updated date, reason reportable, or root cause.

If you hit the retrieve button, a table like the following will come up:

Network Outage Report System - Report List (01/13/2006 - 01/17/2006)									
Ref. Number	Notification Date	Updated Date	Type	Company	Entity Type	Incident Date/Time	Time Zone	Duration Hrs	Du l
06-01362170	01/13/2006 17:16	N/A	Notification	TESTCO	SS7 network provider	01/13/2006 17:00	Eastern	0	
06-01362241	01/13/2006 17:17	N/A	Notification	TESTCO	SS7 network provider	01/13/2006 17:00	Eastern	0	
06-01362472	01/13/2006 17:21	N/A	Notification	TESTCO	SS7 network provider	01/13/2006 17:00	Eastern	0	

Each outage report occupies a row. Every piece of information about the outage is listed. The output can be copied and pasted into Excel for analysis.

2.8 Modify Password

This screen allows you to modify or change your password:

Network Outage - Modify Password

Old Password:

New Password:

Re-type New Password:

NORS will confirm your change of password.

Network Outage Reporting System

Password has been modified.

Use your selected password for future outage reporting.

2.9 *Modify Profile*

This menu item allows you to modify your profile: your name, phone number, email address and/or address. If you choose this menu item the following screen will appear:

Network Outage - Modify User Profile

Name:

Phone Number: Extension:

E-Mail:

Address:

You may change any of the information in your profile.

2.10 *Modify Company ID*

This screen allows outage coordinators to modify or change their Company's ID.

Network Outage - Modify Company ID

Old Company ID:

New Company ID:

Re-type New Company ID:

NORS will confirm the change of Company ID.

2.11 Deactivate User

Outage coordinators can stop access to NORS by one of their company's outage inputters and outage coordinators by selecting this menu item. When this item is selected, the following kind of screen appears:

Network Outage - Deactivate User

UserName:
Name:
User Type:
Phone Number: Extension:
E-Mail:

2.12 User List

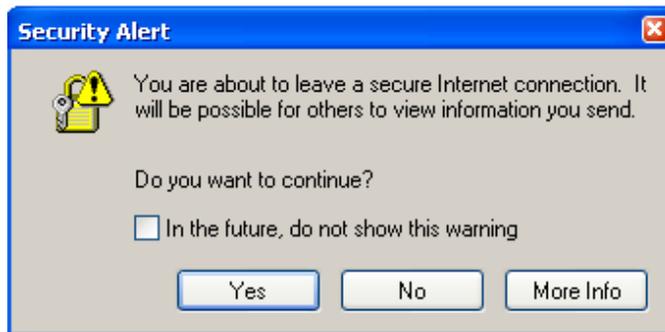
NORS can print out a list of users in spreadsheet format. When you choose this option, the following kind of screen will appear:

List of NORS Users As of 08/20/2008

Name	Username	Type	Phone	Email
Fearless Leader	Flead2	Coordinator	202-418-xxxx	fearless.leader@fcc.gov
TEST USER	testuser	Inputter	202-418-xxxx	test.user@fcc.gov

2.13 XML Filing Utility

This utility will help you to create or edit XML files to be submitted to NORS. There is one self-extractable file (nors_xml.exe) in the directory. When you choose this option, the following dialog box may appear:



If this appears, select “Yes.” Another dialog box will appear:



Save the file to your hard drive and then open it. Four files will be extracted when you do this. “nors.dtd” is the document type definitions file for the NORS. By studying this file, you will see what information needs to be included in the XML file to be submitted to the NORS. The other three files (Setup.Exe, Setup.Ini and Outage_XML_Deployment.msi) can be used to install the .NET utility to help you to create/edit XML files. You also need to download “dotnetfx.exe” (Microsoft .NET Framework Version 1.1 Redistributable Package) from the Microsoft website after verifying that your system meets system requirements for the executing the file:

<http://www.microsoft.com/downloads/details.aspx?familyid=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en>

2.13.1 Creating XML Facility

Once you have downloaded the XML facility and have “dotnetfx.exe” (Microsoft .NET Framework Version 1.1 Redistributable Package), you can create the XML facility. You should execute the file Setup.Exe. This file will create the Outage_XML.exe file. This is the program to easily create XML files.

2.13.2 Creating XML Files

Open the Outage_XML facility. You will be given four choices:

- 1) Create a Notification
- 2) Edit Notification
- 3) Update a Report - This is to change a Notification into an Initial Report (or Draft or Final Report). It can also be used to update an Initial Report or create a Final or Withdrawn Report. You will need the Report ID (from when you submitted the Notification to NORS).
- 4) Exit the System.

Create the file type that you want to upload.

3 Screen for DHS (Retrieve Outage Reports)

The NORS has a module so that DHS can view outages. If you have chosen the retrieval module and successfully logged onto NORS (*see* Section 1.3) thus gaining access to the retrieval module, NORS will display a screen from which you may select an outage to view. DHS can not change any contents of any report.

4 Fields on the Notification Form

Name of Reporting Entity – This 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 inquirer used when he/she applied for a UserID. The Commission requires providers of wireline, wireless, cable circuit-switched telephony, satellite, paging, Signaling System 7 communications services to submit outage reports regarding disruptions to communication when disruptions meet the reporting thresholds as defined in Part 4 of the Commission's Rules on any facilities provided for a fee to one or more unaffiliated entities by radio, wire, cable, satellite, and/or lightguide: two-way voice and/or paging service, and /or SS7 communications.

Type of Entity Reporting Disruption – Pick from the scroll down menu the type of entity your company is relative to the incident being reported. The choices are:

- Wireline carrier
- Wireless carrier
- Cable telephony provider
- Paging provider
- Satellite provider

SS7 network provider
E911 service provider
Facility owner or operator

A carrier that provides SS7 service, E911 service and is a facility owner should identify itself as a wireline carrier. The designation “SS7 network provider” is intended for companies that only provide SS7 service. Similarly the designation “E911 service provider” is for companies that only provide all or some portion of E911 service. The designation “Facility owner or operator” is for companies that are not carriers but own, operate and lease facilities for use in telecommunications. A carrier which provides both wireline and wireless services should choose the designation which most closely relates to the incident being reported.

Date of Incident - Provide the month, day and year at the commencement of the outage. The expected format is mm/dd/yyyy. NORS automatically inserts today’s date, but you can change that by first deleting the entire date, then re-entering the correct date.

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), unless referencing GMT. That is, for 1:00 PM, you should use 1300. The format should be XXXX; that is, do not use a colon (this number should be between 0000 and 2359). In most cases both the physical location of the outage and the majority of the effects are in the same time zone. However, some outages have wide-ranging impacts, which may not be at the physical location of the outage, such as a cut undersea cable. In that case, please provide the time at the end of the undersea cable closest to the US or the local time of the physical outage. You should include more detailed explanations in the Initial or Final Report.

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

- [Alaskan](#)
- Atlantic
- [Central](#)
- Eastern
- ~~Central~~
- [Greenwich Mean Time \(GMT\)](#)
- [Guam](#)
- [Hawaii-Aleutian](#)
- Mountain
- [Other](#)
- Pacific
- ~~Alaskan~~
- ~~Hawaii-Aleutian~~
- ~~Guam~~
- ~~Other~~

Puerto Rico is in the Atlantic Time zone.

Date Outage Determined Reportable - Date on which a company determines that an outage has occurred and meets one or more of the reportable thresholds. This field is voluntary.

Local Time Outage Determined Reportable (24 HR Clock) - Time at which a company determines that an outage has occurred and meets one or more of the reportable. This field is voluntary.

Reason Reportable – Provide the threshold that was crossed that determined that this outage was reportable. If more than one threshold was crossed, please choose the primary reason. Pick from the scroll down menu one of the following:

- Wireline – 900,000 User-Minutes
- Wireless – 900,000 User-Minutes
- Cable Telephony – 900,000 User-Minutes
- MSC
- E911
- Blocked Calls
- 1350 DS3s minutes
- DS3-Simplex Greater than 5 Days
- SS7 - MTP Messages
- Airport
- Other Special Facilities (Military, nuclear, etc.)
- Paging
- Satellite
- Other

E911 Outage Location Effects – For non-E911 outages, leave this field blank. For E911 outages, select from the scroll down menu one of the following:

ALI Location Only Affected – for wireline carriers when location of the caller could not be provided, but the call could be routed to a PSAP.

Phase 2 Only Affected – for wireless outages when Phase 2 location information could not be provided, but the call could be routed to a PSAP.

Phase 1 and Phase 2 Only Affected – for wireless outages when neither Phase 1 nor Phase 2 could be provided, but the call could be routed to a PSAP.

More than Location Affected – for wireline and wireless carriers when the call could not be routed to the appropriate PSAP.

Failure Occurred in Another Company's Network - Check the box if the failure occurred in another company's network.

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

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.

Cable Telephony Users - Provide the number of assigned telephone numbers. If this outage did not affect cable telephony users, please leave this blank.

Satellite Users – Provide the number of satellite users affected (if known).

Number Affected

Blocked Calls – Provide the number of blocked calls. If no calls were blocked, please leave the field blank or enter “0”. If blocked call information is available in only one direction for interoffice facilities that handle traffic in both directions, the total number of blocked calls shall be estimated as twice the number of blocked calls determined for the available direction.

If real time information is not available, providers may provide data for the same day(s) of the week and the same time(s) of day as the outage, covering a time interval not older than 90 days preceding the onset of the outage in an effort to estimate blocked calls. In this case, the number of blocked calls reported should be 3 times the historic carried load.

If, for whatever reason, real-time and historic carried call load data are unavailable to the provider, even after a detailed investigation, the provider must estimate 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 must be available on request. In this case, the estimate of the number of blocked calls reported should be 3 times carried load. The number of blocked calls, if known, should be filled out even if it is not the trigger for an outage being reportable.

Real-Time, Historic Check Box - Check 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 and were out of service for 30 or more minutes, regardless of the services carried on the DS3s or the utilization of the DS3s. DS3s restored to service in fewer than 30 minutes should not be recorded in the box for the number of DS3s. For example, if an outage initially took 576 DS3s out of service, but 384 were restored to service in less than 30 minutes, and only 192 were out of service for 30 minutes or longer; the number of affected DS3s should be recorded as “192”. If some failed DS3s were initially knocked out of service but restored in fewer than 30 minutes, the rapid restoration of those DS3s can be noted in the “Description of Incident” field, but they should not counted in the field for number of DS3s affected.

Count any failed STS3c as 3 DS3s, a failed STS12c as 12 DS3s, etc.

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 of SS7 MTP messages carried on a historical basis. Historic carried SS7 MTP messages should be for the same day(s) of the week and the same time(s) of day as the outage. The information should not be 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. Outages affecting major parts of more than one state should be listed as Multi-State. 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. Please do NOT enter the state in this box. Enter the state abbreviation in the “state” box.

Description of Incident - Provide a narrative that describes the sequence of events leading up to the incident, the steps taken to try and resolve the incident once it had occurred, and the action(s) that finally resolved the incident. This is for the reader to better understand what happened. Include any factors that may have contributed to the duration of the incident, "quick fix" actions that may have resolved or at least mitigated the immediate problem but were not the final, long-term solution, and any other contributing factors. 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 NXX-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

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

5 Fields on the Initial, Draft, and Final Report Forms

Note that all of the data previously filled in are carried forward when updating a report. All fields can be changed to reflect new information except the Report Number, Name of Reporting Entity, Type of Entity, and the Date-Time of the previous submission.

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

Date-Time – Self-explanatory. This field is automatically filled in based on the time of the previous submission for the same report number.

Report Type – Choose the type of report: Initial, Draft or Final. An Initial Report on an outage is due no later than 72 hours after the reporting entity discovered that the outage was reportable, and the Final Report on an outage is due no later than 30 days after the reporting entity discovered that the outage was reportable. A Final Report is due in 30 days even in the event that the outage has not yet been cleared by that time. The Initial Report shall contain all available pertinent information 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, which is the same used by the outage inputter when he/she applied for a UserID. This field is automatically filled in. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, paging provider, [E911 service provider](#), or facility

owner and on any facilities which it owns, operates or leases that experiences an outage that meets the reporting thresholds as defined in Part 4 of the Commission's Rules and Regulations.

Type of Entity Reporting Disruption – Lists company type. This entry is automatically filled with the information taken from the Notification. [Companies are not able to change the entry on the Initial Report regardless of what appears on 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), [unless referencing GMT](#). That is, for 1:00 PM, you should use 1300. The format should be nnnn; do not use a colon (this number should be between 0000 and 2359). In most cases, both the physical location of the outage and the majority of the effects are in the same time zone. However, some outages have wide-ranging impacts that may not be at the physical location of the outage, such as a cut undersea cable. In that case, please provide the time at the end of the undersea cable closest to the US or the local time of the physical outage.

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

- [Alaskan](#)
- Atlantic
- [Central](#)
- Eastern
- ~~Central~~
- [Greenwich Mean Time \(GMT\)](#)
- [Guam](#)
- [Hawaii-Aleutian](#)
- Mountain
- [Other](#)
- Pacific
- ~~Alaskan~~
- ~~Hawaii-Aleutian~~

~~Guam~~
~~Other~~

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

Reason Reportable – Provide the threshold that was crossed that determined that this outage was reportable. If more than one threshold was crossed, please choose the primary reason. Pick from the scroll down menu one of the following:

Wireline – 900,000 User-Minutes
Wireless – 900,000 User-Minutes
Cable Telephony – 900,000 User-Minutes
MSC
E911
Blocked Calls
1350 DS3s minutes
DS3-Simplex Greater than 5 Days
SS7 - MTP Messages
Airport
Other Special Facilities (Military, nuclear, etc.)
Paging
Satellite
Other

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 includes the restoration of all services to all customers impacted by the outage, even if the restoral is over temporary facilities. If the customers' locations are destroyed such as by a hurricane, flood, tornado, or wildfire the duration continues until the reporting carrier is capable of again providing service to those locations. If an outage is ongoing at the time the Final Report is filed, report the outage duration as the total time between the commencement of the outage and the time the Final Report is filed.

Date Outage Determined Reportable - Date on which a company determines that an outage has occurred and meets one or more of the reportable thresholds. This field is voluntary.

Local Time Outage Determined Reportable (24 HR Clock) - Time at which a company determines that an outage has occurred and meets one or more of the reportable. This field is voluntary.

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, provide information on the number of users in each block restored to service and the elapsed time to partial 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. In addition, for outages that last an unusually long time, an explanation should be provided in this field.

Inside Building Indicator – Indicate whether the outage occurred inside a building owned, leased, or otherwise controlled by the reporting entity. A building is a structure that is temperature controlled.

E911 Outage Location Effects – For non-E911 outages, leave this field blank. For E911 outages, select from the scroll down menu one of the following:

ALI Location Only Affected – for wireline carriers, when location of the caller could not be provided but the call could be routed to a PSAP.

Phase 2 Only Affected – for wireless outages, when Phase 2 location information could not be provided but the call could be routed to a PSAP.

Phase 1 and Phase 2 Only Affected – for wireless outages, when neither Phase 1 nor Phase 2 could be provided but the call could be routed to a PSAP.

More than Location Affected – for wireline and wireless carriers, when the call could not be routed to the appropriate PSAP.

Failure Occurred in Another Company's Network - Check the box if the failure occurred in another company's network.

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 outages where only intraLATA service or only 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. In determining the number of users potentially affected by a failure of a switch, a concentration ratio of 8 shall be applied. If this outage did not affect wireless users, please leave this blank.

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.

Cable Telephony Users - Provide the number of assigned telephone numbers. If this outage did not affect cable telephony users, please leave this blank.

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 leave the field blank or put 0 down. If blocked call information is available in only one direction for interoffice facilities which handle traffic in both directions, the total number of blocked calls shall be estimated as twice the number of blocked calls determined for the available direction.

If real time information is not available, providers may provide data for the same day(s) of the week and the same time(s) of day as the outage, covering a time interval not older than 90 days preceding the onset of the outage in an effort to estimate blocked calls. In this case, the number of blocked calls reported should be 3 times the historic carried load.

If, for whatever reason, real-time and historic carried call load data are unavailable to the provider, even after a detailed investigation, the provider must estimate 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 must be available on request. In this case, the estimate of the number of blocked calls reported should be 3 times

carried load. The number of blocked calls, if known, must be filled out even if it is not the trigger for an outage being reportable.

Real-Time, Historic Check Box - Check whether the number of Blocked Calls came from real-time data or was based on historic loads carried 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 and were out of service for 30 or more minutes, regardless of the services carried on the DS3s or the utilization of the DS3s. DS3s restored to service in fewer than 30 minutes should not be recorded in the box for the number of DS3s. For example, if an outage initially took 576 DS3s out of service, but 384 were restored to service in less than 30 minutes, and only 192 were out of service for 30 minutes or longer; the number of affected DS3s should be recorded as “192”. If some failed DS3s were initially knocked out of service but restored in fewer than 30 minutes, the rapid restoration of those DS3s can be noted in the “Description of Incident” field, but they should not counted in the field for number of DS3s affected.

Count any failed STS3c as 3 DS3s, a failed STS12c as 12 DS3s, etc.

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 should be for the same day(s) of the week and the same time(s) of day as the outage. The information should not be 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. 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. Please do NOT enter the state in this box. Enter the state in the “state” box.

More Complete Description of Geographical Area of Outage – Provide a more complete description of the geographical area of the outage. In particular, for Multi-State outages, 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 that describes the sequence of events leading up to the incident, the steps taken to try and resolve the incident once it had occurred, and the action(s) that finally resolved the incident. This is for the reader to better understand what happened. Include any factors that may have contributed to the duration of the incident, "quick fix" actions that may have resolved or at least mitigated the immediate problem but were not the final, long-term solution, and any other contributing factors. The description should be sufficiently detailed to allow the reader to reach the same conclusions as the writer as to the Direct Cause and Root Cause of the incident. The maximum number of characters that will be saved in this field is [blank]. Additional text may be referenced here and placed in the remarks field. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg4]: The FCC will need to identify the number of these characters.

Comment [rg5]: The FCC will need to identify what these special characters are.

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 ~~imputer's~~ inputter's own words and should not use the words in the pull-down menus for Direct Cause or Root Cause. The following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg6]: The FCC will need to identify what these special characters are.

Direct Cause: The direct cause is the immediate event that results in an outage – Scroll down the menu and choose the direct cause that is the most accurate. The direct cause is the event, action, or procedure that triggered the outage. In Section 7, there is a complete description of each of the direct causes. For example, a cable cut could be the triggering event or direct cause of an outage whose root cause is lack of diversity.

Root Cause: The root cause is the underlying reason why the outage occurred or why the outage was reportable. – Scroll down the menu and ~~pick~~ choose the root cause that best fits. Root Cause is the key problem which once identified and corrected will prevent the same or a similar problem from recurring. With 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 cause - the Root Cause. In Section 7, there is a complete description of each root cause. For example, a cable cut improper marking could be the triggering event or direct cause but the real cause (root cause) may be lack of diversity.

Contributing Factors – Scroll down the menu and ~~pick~~ choose the contributing factors that best fit, if applicable. Contributing factors are problems or causes that are closely linked to the outage. Often if a contributing factor ~~were~~ was addressed beforehand, the outage could have been prevented or the effect of the outage would have been reduced or eliminated. The form allows two contributing factors, for which there are complete descriptions in Section 7.

Lack of Diversity Contributed to, or Caused, the Outage – Determine whether lack of diversity contributed to or caused the outage. If Best Practices related to diversity are discussed in any of the Best Practice fields, or if the lack of diversity is listed as a root

cause or contributing factor to the outage, then this field should be marked “Yes”. In general, determine whether engineering standards for diversity are being followed.

Malicious Activity – Indicate whether you believe that malicious activity might be involved in the outage. The form asks for some explanation of why you believe the activity is malicious or what is suspicious about the activity. Malicious activity could be the product of terrorists. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg7]: The FCC will need to identify what these special characters are.

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, then report the make and model of the relay, not the power plant or switch.

Specific Part of the Network Involved – Provide the part of the network involved with the incident. 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. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg8]: The FCC will need to identify what these special characters are.

Telecommunications Service Priority (TSP) Indicator – Indicate whether TSP was ~~provided~~ involved during service restoration.

Steps Taken to Prevent Reoccurrence – Provide the steps already taken and to be taken to prevent reoccurrence. Typically, the corrective actions are identified through a Root Cause Analysis of the incident and the steps for prevention can be at both this location and throughout the network(s) if appropriate. 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. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg9]: The FCC will need to identify what these special characters are.

Applicable Best Practices that might have prevented the Outage or reduced its effects – Provide the number(s) ~~and also possibly descriptions~~ of the Best Practices that could have prevented the outage or reduced its effects. The Network Reliability and Interoperability Council (NRI) and Communications Security, Reliability, and Interoperability Council (CSRIC) ~~have~~ has developed a list of Best Practices. They can be accessed via www.nric.org or <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm>. You can find relevant Best Practices by using keywords. Alternatively, Best Practices can also be sourced from the ATIS Best Practices website: <http://www.atis.org/bestpractices>.

Best Practices used to diminish effects of the Outage - Provide the number(s) and also possibly descriptions of the most important Best Practices that were actually used to lessen the effects of the outage. These chosen Best Practices helped shorten the outage, reduced the restoration times, prevented the outage from affecting more customers, and/or reduced the effects on customers (e.g., ensured that E911 was not affected). If none were used, please leave blank. [Best Practices can be sourced from the https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm](https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm) or <http://www.atis.org/bestpractices>.

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. [Also, the following special characters \[blank\] may not be used in any text fields as they will prevent the outage Report from being saved.](#)

Comment [rg10]: The FCC will need to identify what these special characters are.

Remarks – Provide any additional information that you believe is relevant, but did not fit anywhere else on the form. [Also, the following special characters \[blank\] may not be used in any text fields as they will prevent the outage Report from being saved.](#)

Comment [rg11]: The FCC will need to identify what these special characters are.

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 ~~NXX~~NPA-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

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 ~~NXX~~NPA-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

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.

6 Fields on the Withdrawn Report 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 [NXXNPA](#)-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

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

U.S. Postal Service Address – Provide the 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 [NXXNPA](#)-NXX-XXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide the extension number, if used, in format XXXX.

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

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

Reason for Withdrawal – State the reason that the report is being withdrawn.

7 Descriptions of Root Cause, Direct Cause and Contributing Factors

Cable Damage

Cable Unlocated

This is considered a procedural error. Prior notification of action 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.

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).

Inaccurate/ Incomplete Cable Locate

This is considered a procedural error. The cable's presence was determined, but its location was inaccurately and/or partially identified.

Inadequate/No Notification

Excavator failed to provide sufficient or any notification prior to digging, did not accurately describe the location of the digging work to be performed, or did not wait the required time for locate completion.

Other

Shallow Cable

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

Cable Damage/Malfunction

Aerial/Non-Buried

Aerial/non-buried cable was damaged or ceased to function (e.g., power transformer fire, tension on span, automobile collision, etc.).

Cable Malfunction

Cable ceased to function (e.g., loss of transmission due to aging, connector failure, etc.).

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.

Other

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.

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; software vulnerability to virus infection.

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 resulting from the removal of a good unit with restoral of faulty mate; failure to switch/protect the switch to standby/spare/mate component(s).

Other

Diversity Failure

External

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

Internal (Other)

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

Links

SS7 communication paths were not physically and logically diverse.

Power

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

Timing Equipment

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

Environment – External (for limited use when applicable root causes caused by a service provider or vendor cannot be identified; it can also be listed as contributing factor).

Animal Damage

Component destruction associated with damage caused by animals (e.g., squirrel/rodent chewing of cables, insect infestation, bird droppings, bird nests, etc.).

Earthquake

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

Fire

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

Flood

Ice/Storm

Lightning/Transient Voltage

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

Other

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 vehicle (car, truck, train, etc.) collision.

Formatted: Indent: Left: 0.5", First line: 0"

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/lack of response to (alarmed/un-alarmed) environmental failures, or due to incorrect manual control of environmental systems, consider this a procedural fault.

Fire Suppression (water, chemicals) Damage

Component loss or fault associated with corrosion (electrolytic or other) caused by fire suppression activities; this root cause assumes that 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).

Manhole/Cable Vault Leak

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

Other

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.

Hardware Failure

Circuit Pack/Card Failure-Other

Circuit pack or card, other than within the processor, failed (e.g., component failure, pin edge connector failure, firmware failure, etc.).

Circuit Pack/Card Failure-Processor

Circuit pack or card within the processor failed (e.g. component failure, pin edge connector failure, firmware failure, etc.).

Memory Unit Failure

Other**Passive Devices**

Equipment, hardware or devices that contain no electronics (e.g., demarcation points, cross connect panels, splitters, attenuators, etc.).

Peripheral Unit Failure**Processor Community Failure****Self-contained Device Failure**

Equipment or hardware that contains electronics, but does not contain replaceable components.

Shelf/Slot Failure

Failure of entire equipment shelf/chassis, connectors, or backplane (e.g., physical damage, corrosion, contamination, wear, etc.).

Software Storage Media Failure

Hardware failure resulting in corruption of office data, program data, routing data, etc.

Insufficient Data**Insufficient Data “Blank”**

There is not enough information from the failure report (and subsequent investigation, if any) to determine cause(s) of failure.

Cleared While Testing

Service restored before the cause could be determined.

Non-Service Provider Personnel

Failure is caused by non-service provider personnel (e.g., contractors, building maintenance personnel, tenant of telco hotel, etc.).

Outside Owned Network

Failure occurred in another company’s network (e.g., leased transport capacity, contracted signaling service, etc.).

Under Investigation

Root cause analysis pending.

Other/Unknown

Insufficient data available due to a reason not noted above.

Other/Unknown

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Excludes 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 the probable cause, which falls under the heading "unknown." When classifications provided do not match the cause, the approximate match is preferred to be "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.

Breaker Tripped/Blown Fuses

Equipment Failure associated with tripped breaker or blown fuse.

Extended Commercial Power Failure

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

Generator Failure

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

Inadequate Site-Specific Power Contingency Plans

System failure due to the insufficiency of the emergency operating procedures and contingency plans available and the resulting outage is prolonged because of lack of site-specific information. This includes equipment engineering data, portable engine hook-up hardware/procedures, load shedding plans, etc.

Inadequate Back-up Power Equipment Located on Customer Premise

Customer premise power equipment unable to support communications equipment due to extended loss of commercial or back-up power.

Inadequate/Missing Power Alarm

System failure associated to an un-alarmed (or under-alarmed) power failure, an alarm not provided initially due to inadequate standards, failure to implement standards or an 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. Consider this a procedural fault.

Lack of Power Redundancy

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

Lack of Routine Maintenance/Testing

System failure resulting from infrequent power system testing, maintenance and/or detailed inspection. Consider this a procedural fault.

Other

Overloaded/Undersized Power Equipment

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

Rectifier Failure

System failure resulting from rectifier malfunction.

Scheduled Activity-Software Upgrade

Scheduled Maintenance-Hardware Replacement

Unidentified Power Surge

Equipment failure associated with unidentified power surge.

Procedural - Other Vendor/Contractor

Ad hoc Activities, Outside Scope of MOP

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

Documentation/Procedures Out-of-Date, Unusable, Impractical

Lack of updated documentation/procedures, the correction/update is available but not incorporated locally, or the document is unwieldy. Some examples are: the use of inadequate indexing or cross-referencing, bits and pieces of information being too difficult to integrate, ineffective delivery vehicle, etc.

Documentation/Procedures Unavailable, Incomplete

Documentation or procedures (vendor or service provider) are not published; published, but not distributed; distributed, but not available on-site; or that some documentation is obscure/oblique, too general (lack of practical detail); too detailed/technical for practical use, etc.

Insufficient Staffing/Support

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 or Employee Error

Resulting from insufficient leadership, ineffective administration, and/or maintenance strategies (process or communication failures; conflicting priorities) etc. This sub-category should be used when multiple procedural causes are indicated, and also when the service interruption results purely from an unintentional action by the employee.

Insufficient Training

Training not available from vendor; training not available from service provider; training available but not attended; training attended but provides inadequate or out-of-date information; 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 are not updated; correction/update available, but not incorporated locally. Documentation/procedures are 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) are not published; published, but not distributed; distributed, but not available on-site, etc.

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

Inadequate Routine Maintenance/Memory Back-Up

Failure could have been prevented/minimized by simple maintenance routines. The resulting recovery action was delayed/complicated by old or missing program/office data tapes or disk, etc.

Insufficient Staffing/ Support

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 or Employee Error

Resulting from insufficient leadership, ineffective administration, and/or maintenance strategies (process or communication failures; conflicting priorities), etc. This sub-category should be used when multiple procedural causes are indicated, and also when the service interruption results purely from an unintentional action by the employee.

Insufficient Training

Training not available from vendor; training not available from service provider; training available but not attended; training attended but provides inadequate or out-of-date information; 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 or Impractical

Documentation/procedures are not updated; correction/update available, but not incorporated locally. Documentation/procedures are 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) are not published; published, but not distributed; distributed, but not available on-site, etc.

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

Insufficient Staffing/ Support

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 or Employee Error

Resulting from insufficient leadership, ineffective administration, and/or maintenance strategies (process or communication failures; conflicting priorities) etc. This sub-category should be used when multiple procedural causes are indicated, and also when the service interruption results purely from an unintentional action by the employee.

Insufficient Training

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

Other

Simplex Condition

Non-service Affecting

Occurs when there is a failure of one side of a duplexed system such as a SONET ring yet an unprotected simplex service will still provide service for the duration of the outage. Do not use this root cause for the complete failure of a duplexed system or in cases where any of the circuits in the duplexed system are provided under SLAs which require protection.

Service Affecting

Failure of one side of a duplexed system such as a SONET ring where an unprotected simplex service was provided for a period of time but was not repaired during the usual maintenance window or in cases where any of the circuits in the duplexed system are provided under SLAs that require protection.

Spare

Spare Not Available – Sparing processes did not result in an available replacement (e.g., Service Provider inventory inaccuracies, transportation of spare located at centralized facility, etc.).

Spare On Hand – Failed

Sparing processes provided an available replacement; however, the replacement malfunctioned (e.g., out-of-box failure of spare, incompatible software versions, etc.).

Spare On Hand – Manufacturer Discontinued (MD)

Obtaining spare made difficult or complicated by MD'd status (e.g., Service Provider unaware of MD'd status, scarcity of MD's spares, etc.).

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 the 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., then consider the problem to be a software design fault.

Inappropriate/Insufficient Network Management (NM) Control(s)

System/network overload or congestion associated with an ineffective NM system/switch response resulting due to the lack of either effective NM control, that the system/switch response to control was inappropriate, or that its implementation was flawed. If failure was related to inappropriate control strategy or execution by NM organization, consider it procedural.

Ineffective Engineering/Engineering Tools

System/network overload or 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 it procedural.

Mass Calling - Focused/Diffuse Network Overload

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

Media-Stimulated Calling - Insufficient Notification

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

Other

Report Type

Choose the type of report: Initial, Draft or Final. ~~An Initial Report is due within 2 days of the on an outage. Final Reports are due within 30 days of is due no later than 72 hours after the reporting entity discovered that~~ the outage ~~from when~~ was reportable, and the ~~Final Report on an outage started~~ is due no later than 30 days after the reporting entity discovered that the outage was reportable. A Final Report is due in 30 days even in the event that the outage has not yet been cleared by that time. The Initial Report shall contain all available 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. ~~which This field is automatically filled in. It is the name of the company that same used by~~ the outage inputter ~~used~~ when he/she applied for a UserID. This field is automatically filled in. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, paging provider, E911 service provider, or facility owner and on any facilities which it owns, operates or leases that experiences an outage ~~meeting that meets~~ 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~~ type. This entry is automatically filled with the information taken from the Notification. Companies are not able to change the entry on the Initial Report regardless of what appears on 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), unless referencing GMT. 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 (this~~ number should be between ~~0000~~ and ~~2359~~~~In~~2359). In most cases, both the physical location of the outage and the majority of the effects ~~of the outage~~ are in the same time zone. However, some outages have wide-ranging impacts ~~and at times the greatest customer impact that~~ may not be at the physical location of the outage. ~~For undersea cables, such as a cut, undersea cable. In that case, please~~ provide the time at the ~~closest~~ end of the undersea cable closest to the US. ~~Detailed explanations will be provided in the Initial or Final Report. the local time of the physical outage.~~

Time Zone

Pick from the scroll down menu one of the following:

- Alaskan
- Atlantic
- Central
- Eastern
- Greenwich Mean Time (GMT)
- Guam
- Hawaii-Aleutian
- Mountain
- Other
- Pacific

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

Reason Reportable

Provide the threshold that was crossed that determined that this outage was reportable. If more than one threshold was crossed, please choose the primary reason. Pick from the scroll down menu one of the following:

- [Wireline – 900,000 User-Minutes](#)
- [Wireless – 900,000 User-Minutes](#)
- [Cable Telephony – 900,000 User-Minutes](#)
- [MSC](#)
- [E911](#)
- [Blocked Calls](#)
- [1350 DS3s minutes](#)
- [DS3-Simplex Greater than 5 Days](#)
- [SS7 - MTP Messages](#)
- [Airport](#)
- [Other Special Facilities \(Military, nuclear, etc.\)](#)
- [Paging](#)
- [Satellite](#)
- [Other](#)

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 includes the~~ restoration of ~~service~~all services to all customers impacted by the outage, ~~not only restoration of the service(s) which may have made~~ even if the restoral is over temporary facilities. If the customers' locations are destroyed such as by a hurricane, flood, tornado, or wildfire the duration continues until the reporting carrier is capable of again providing service to those locations. If an outage reportable to the FCC is ongoing at the time the Final Report is filed, report the outage duration as the total time between the commencement of the outage and the time the Final Report is filed.

Date Outage Determined Reportable

Date on which a company determines that an outage has occurred and meets one or more of the reportable thresholds. This field is voluntary.

Local Time Outage Determined Reportable (24 HR Clock)

Time at which a company determines that an outage has occurred and meets one or more of the reportable. This field is voluntary.

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, provide information on the number of users in ~~the~~each 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. In addition, for outages that last an unusually long time, an explanation should be provided in this field.

Inside Building Indicator

Indicate whether the outage occurred inside a building owned, leased, or otherwise controlled by the reporting entity. ~~Outages that occur on fiber facilities or in fiber huts are considered outside a building. A building is a structure that is temperature controlled.~~

E911 Outage Location Effects

For non-E911 outages, leave this field blank. For E911 outages, select from the scroll down menu one of the following:

ALI Location Only Affected – for wireline carriers, when location of the caller could not be provided but the call could be routed to a PSAP.

Phase 2 Only Affected – for wireless outages, when Phase 2 location information could not be provided but the call could be routed to a PSAP.

Phase 1 and Phase 2 Only Affected – for wireless outages, when neither Phase 1 nor Phase 2 could be provided but the call could be routed to a PSAP.

More than Location Affected – for wireline and wireless carriers, when the call could not be routed to the appropriate PSAP.

Failure Occurred in Another Company's Network

Check the box if the failure occurred in another company's network.

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. If this outage did not affect wireless users, please leave this blank.

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. 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 Affected:

Blocked Calls

Provide the number of blocked calls. If no calls were blocked, please leave the field blank or put 0 down. ~~For~~ If blocked call information is available in only one direction 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~~

If real time information is not available, providers may ~~use historic carried call load~~ provide data for the same day(s) of the week and the same time(s) of day as the outage, ~~and for covering~~ a time interval not older than 90 days preceding the onset of the outage; in an effort 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 the historic carried load. ~~In situations where~~

If, 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~~ estimate the carried call load based on data obtained in the time interval between the ~~onset~~ repair of the outage and the due date for the ~~final report~~ 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 estimate of the number of blocked calls reported should be 3 times carried load. The number of blocked calls ~~should, if known, must~~ 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~~ Blocked Calls came from real-time data or was based on historic loads 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 DS3 circuits that were affected by the outage.~~ Provide the number of previously operating DS3s that were affected by the outage and were out of service for 30 or more minutes, regardless of the services carried on the DS3s or the utilization of the DS3s. DS3s restored to service in fewer than 30 minutes should not be recorded in the box for the number of DS3s. For example, if an outage initially took 576 DS3s out of service, but 384 were restored to service in less than 30 minutes, and only 192 were out of service for 30 minutes or longer; the number of affected DS3s should be recorded as "192". If some failed DS3s were initially knocked out of service but restored in fewer than 30 minutes, the rapid restoration of those DS3s can be noted in the "Description of Incident" field, but they should not counted in the field for number of DS3s affected.

Count any failed STS3c as 3 DS3s, a failed STS12c as 12 DS3s, etc.

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 shallshould be for the same day(s) of the week and the same time(s) of day as the outage, ~~and for a time interval.~~ The information should not be 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~~ Outages affecting major parts of more than one state should be listed as ~~multi-state.~~ 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. Please do NOT enter the state in this box. Enter the state in the "state" box.

More Complete Description of Geographical Area of Outage

Provide a more complete description of the geographical area of the outage. In particular, for ~~widespread~~ Multi-State 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~~ that describes the sequence of events leading up to the incident, the steps taken to try and resolve the incident once it had occurred, and the action(s) ~~which~~ that finally ~~brought resolution to~~ resolved the incident. This is for the reader to better understand what happened. Include any factors ~~which~~ that may have contributed to the duration of the incident, "quick fix" actions ~~which~~ that may have resolved or at least mitigated 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. ~~The maximum number of characters that will be saved in this field is [blank]. Additional text may be referenced here and placed in the remarks field. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.~~

Comment [rg1]: The FCC will need to identify the number of these characters.

Comment [rg2]: The FCC will need to identify what these special characters are.

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 ~~inputter's~~ own words ~~of outage inputter~~ and should not ~~necessarily~~ use the words ~~contained~~ in the pull-down menus: for Direct Cause or Root Cause. ~~The following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.~~

Comment [rg3]: The FCC will need to identify what these special characters are.

Direct Cause: The direct cause is the immediate event that results in an outage

Scroll down the menu and ~~pick~~choose the direct cause that ~~fits best is the most accurate.~~ The direct cause is the event, action, or procedure that triggered the outage. ~~In the Appendix~~Section 7 ~~of the NORS User Manual,~~ there is a complete description of each of the direct causes. For example, a cable cut ~~is often could be~~ the triggering event or direct cause ~~but the real cause or of an outage whose~~ root cause ~~may be is~~ lack of diversity.

- None
- 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).~~
 - ~~Inaccurate/ Incomplete cable locate—The cable's presence was determined, but their locations were inaccurately identified. 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 rectifierschargers, 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 rectifiers/chargers, 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~~

Root Cause: The root cause is the underlying reason why the outage occurred or why the outage was reportable

Scroll down the menu and pick-choose the root cause that best fits best. Root Cause is the key problem, which once identified and corrected, would will prevent the same or a similar problem from recurring. ~~In~~ With 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-cause - the Root Cause. ~~In the Appendix~~ Section 7, there is a complete description of each ~~of the~~ root causes-cause. For example, a cable cut is often improper marking could be the triggering event or direct cause but the real cause or (root cause) may be lack of diversity.

- ~~None~~
- ~~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 rectifiers/chargers, 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

Contributing Factors

Scroll down the menu and pick-choose the contributing factors that fit-best- fit, if applicable. Contributing factors are problems or causes that are closely linked to the outage. Often if a contributing factor were-was addressed beforehand, the outage could be-have been prevented or the effect of the outage would have been reduced or eliminated. The form allows two contributing factors-, [for which there are complete descriptions in Section 7 of the NORS User Manual](#).

- ~~None~~
- ~~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 rectifiers/chargers, battery power plant, 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~~

Diversity Indicator Lack of Diversity Contributed to, or Caused, the Outage

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 ~~the~~ lack of diversity is listed as a root cause or contributing factor to the outage, then ~~the diversity checkbox must also~~ this field should be checked-marked “Yes”. ~~In general, determine whether engineering standards for diversity are being followed.~~

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~~ The form asks for some explanation of why ~~the in putter believes you believe~~ the activity is malicious or what is suspicious about the activity. ~~Malicious activity could be the product of terrorists. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.~~

Comment [rg4]: The FCC will need to identify what these special characters are.

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, then report the make and model of the relay, not the power plant or switch.

Specific Part of the Network Involved

Provide the part of the network involved- with the incident. 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. ~~If Telecommunications Service Priority was used to restore service, include how it was used. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.~~

Comment [rg5]: The FCC will need to identify what these special characters are.

Telecommunications Service Priority (TSP) Indicator

Indicate whether TSP was ~~used~~ involved 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, ~~and the steps for prevention can be at both this location and throughout the network(s) if appropriate.~~ 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. ~~Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.~~

Comment [rg6]: The FCC will need to identify what these special characters are.

Applicable Best Practices that might have prevented the Outage or reduced its effects

Provide ~~a description~~ the number(s) of the Best Practices that could have prevented the outage or reduced its effects. The Network Reliability and Interoperability Council (NRI) and Communications Security, Reliability, and Interoperability Council (CSRIC) has have developed a list of Best Practices. They can be accessed via ~~www.nrie.org~~ or https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm. You can find relevant Best Practices by using keywords. Alternatively, Best Practices can also be sourced from the ATIS Best Practices website: http://www.atis.org/bestpractices.

Formatted: Not Highlight

Formatted: Not Highlight

Best Practices used to ~~mitigate~~ diminish effects of the Outage

Provide ~~a description of the number(s)~~ and also possibly descriptions of the most important Best Practices that were actually used to ~~mitigate~~ lessen the effects of the outage. These chosen Best ~~practices~~ Practices helped shorten the outage, reduced the restoration times, prevented the outage from affecting more customers, and/or reduced the effects on customers (e.g., ensured that E911 was not affected). If none were used, please leave blank. Best Practices can be sourced from https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm or the ATIS Best Practices website: http://www.atis.org/bestpractices. and from or.

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~~. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg7]: The FCC will need to identify what these special characters are.

Remarks

Provide any additional information that you believe is relevant, ~~but that~~ did not fit anywhere else on the form. Also, the following special characters [blank] may not be used in any text fields as they will prevent the outage Report from being saved.

Comment [rg8]: The FCC will need to identify what these special characters are.

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 ~~###NPA-###NXX-###XXXX~~. That is, 201-444-5656 would mean that the area code or NPA is 201, the NNX is 444, and the line number is 5656.

Extension

Provide the extension number, if used, in format ~~###XXXX~~.

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 ~~###NPA-###NXX-###XXXX~~. That is, 201-444-5656 would mean that the area code or NPA is 201, the NNX is 444, and the line number is 5656.

Extension

Provide the extension number in format ~~###XXXX~~.

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.

Reason Reportable

Provide the reason why this outage is reportable.

Real Time, Historic Check Box

Mobile Switching Center (MSC) Failed

TBD.

E911 Outage – Location Affects

TBD.

Failure Occurred in Another Companies Network

TBD.