



1200 G Street, NW  
Suite 500  
Washington, DC 20005

P: 202-628-6380  
F: 202-393-5453  
W: [www.atis.org](http://www.atis.org)

ATIS Board Officers

Chair  
**Kristin Rinne**  
AT&T

First Vice Chair  
**Stephen Bye**  
Sprint

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, 2013

**Via Email**

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

Re: ATIS NRSC Recommendations for NORS Help File

Dear Jeff:

Attached are recommendations from the ATIS Network Reliability Steering Committee (NRSC) for changes to the Network Outage Reporting System (NORS) Help File (a clean and marked up version are attached). These changes align the text with what is currently contained in the NORS and associated NORS User Manual Version 7.


In addition to the recommended changes, there are three observations noted as comments in the attached:

- The first comment pertains to whether there should be a VoIP service provider bullet added to the list of company types under the "Type of Entity Reporting Disruption" section. If the answer to this question is "yes," the NRSC recommends that this be addressed in the NORS production system and NORS User Manual.
- The second comment notes that the "Mobile Switching Center (MSC) Failed" appears only in the online reporting system, but is not documented in the Help File or NORS User Manual. The NRSC recommends that this section heading be added to the Help File and the User Manual.
- The third comment recommends updating the NORS User Manual to reflect the changes proposed by the NRSC to the "State" section of the Help File, which has been renamed as "Geographic Area Affected State, Territory, Commonwealth, or the District of Columbia" to reflect what is currently displayed on the online reporting system.

Letter to J. Goldthorp  
July 19, 2013  
Page 2

Thank you for your consideration of these items. Please contact me if additional information is necessary, or if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas Goode". The signature is fluid and cursive, with the first name "Thomas" being more prominent than the last name "Goode".

Thomas Goode  
General Counsel

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

### 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. An Initial Report is not required if VoIP is the only service affected.

---

### 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, Voice over Internet Protocol (VoIP) 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

**Comment [RG1]:** NRSC Comment: Should there be a VoIP service provider bullet added to this list? If so, this needs to be addressed in the NORS production system and NORS User Manual.

---

### **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). 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. 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
- Greenwich Mean Time (GMT)
- Guam
- Hawaii-Aleutian
- Mountain
- Other
- Pacific

Puerto Rico is in the Atlantic Time zone.

---

### **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
- VoIP – E911
- VoIP – 900,000 User-Minutes

---

### **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 restoration 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.

**VoIP**

Check the box if VoIP 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. 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.

#### **VoIP Users**

Provide the number of potentially affected VoIP users. If this outage did not affect VoIP 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 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 be 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.

### **Mobile Switching Center (MSC) Failed**

**Comment [RG2]:** NRSC Comment: The MSC section appears only in NORS, but not the NORS User Manual or the Help File. Recommended adding this section heading.

### **Geographic Area Affected**

#### **State, Territory, Commonwealth, or the District of Columbia**

**Comment [RG3]:** NRSC Comment: The heading of this section needs to be updated in the NORS User Manual as well.

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 5,000, and that may be reduced due to the way words break at the end of a line in the field. Additional text may be referenced here and placed in the remarks field.

#### **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 and should not use the words in the pull-down menus for Direct Cause or Root Cause.

**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 of the NORS User Manual, 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 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 of the NORS User Manual, 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.

o

**Contributing Factors**

Scroll down the menu and 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 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 of the NORS User Manual.

**~~Diversity Indicator~~ 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.

---

### **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.

### **Telecommunications Service Priority (TSP) Indicator**

Indicate whether TSP was 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.

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

Provide the number(s) of the Best Practices that could have prevented the outage or reduced its effects. The Network Reliability and Interoperability Council (NRIC) and Communications Security, Reliability, and Interoperability Council (CSRIC) have developed a list of Best Practices. They can be accessed via <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 <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.

### **Remarks**

Provide any additional information that you believe is relevant, but did not fit anywhere else on the form.

### **Primary Contact Person**

Provide the full name of the primary contact person.

### **Phone Number**

Provide the phone number of the primary contact person in the format 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.

## Report Type

Choose the type of report: Initial, Draft or Final. ~~An Initial Reports are 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. An Initial Report is not required if VoIP is the only service affected.

## 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, Voice over Internet Protocol (VoIP) 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

**Comment [RG1]:** NRSC Comment: Should there be a VoIP service provider bullet added to this list? If so, this needs to be addressed in the NORS production system and NORS User Manual.

---

### 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). 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. 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
- 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  
VoIP – E911  
VoIP – 900,000 User-Minutes

---

### **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:

*ALL 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.

**VoIP**

Check the box if VoIP 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.

**VoIP Users**

Provide the number of potentially affected VoIP users. If this outage did not affect VoIP 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 ~~shall~~ should 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.

#### Mobile Switching Center (MSC) Failed

**Comment [RG2]:** NRSC Comment: The MSC section appears only in NORS, but not the NORS User Manual or the Help File. Recommended adding this section heading.

**Formatted:** Font color: Red

#### Geographic Area Affected

##### State, Territory, Commonwealth, or the District of Columbia

**Comment [RG3]:** NRSC Comment: The heading of this section needs to be updated in the NORS User Manual as well.

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 5,000, and that may be reduced due to the way words break at the end of a line in the field. 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.

### 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.

#### **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 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

**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 of the NORS User Manual](#), 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 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~~

**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~~ 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 inpu~~ the inpu ~~ttter 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.~~

---

### **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.~~

### **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.~~

### **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 (NRIC) and Communications Security, Reliability, and Interoperability Council (CSRIC) ~~has~~ have 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 ~~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.

### **Remarks**

Provide any additional information that you believe is relevant, but that did not fit anywhere else on the form.

### **Primary Contact Person**

Provide the full name of the primary contact person.

### **Phone Number**

Provide the phone number of the primary contact person in the format ###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 ~~nnnn~~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 ~~nnn~~NPA-~~nnn~~NNX-~~nnnn~~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 ~~nnnn~~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: