Network Outage Reporting System Information Sharing User Manual

Version 1

September 2022

Table of Contents

Table of Figures

1. Introduction

In 2004, the Federal Communications Commission (FCC) adopted rules that require outage reporting for communications providers (including wireline, wireless, paging, cable, satellite, VoIP, and Signaling System 7 service providers), to address the critical need for rapid, complete, and accurate information on service disruptions that could affect homeland security, public health or safety, and the economic well-being of our Nation. These outage reports are filed in the FCC's Network Outage Reporting System (NORS).

The FCC shares the communications outage information collected in NORS with state, federal, and Tribal nation agencies to improve their situational awareness, enhance their ability to respond more rapidly to outages, and to help save lives, while safeguarding the confidentiality of this data. This User Manual is a step-by-step document to help users easily use NORS.

2. Roles and Privileges

By regulation, access to NORS is limited to acting on behalf of the federal government, the 50 states, the District of Columbia, Tribal Nations, and the U.S. Territories. These agencies must meet the criteria for eligibility before being granted NORS access. To be eligible, an agency must demonstrate its "need to know" by citing to statutes or other regulatory authority that establishes it has official duties making it directly responsible for emergency management and first responder support functions. Agencies meeting these criteria are "Participating Agencies."

The information obtained by Participating Agencies from the databases can only be used for valid public safety purposes i.e., carrying out emergency management and first responder support functions that an agency is directly responsible for pursuant to its official duties.

Participating Agencies must preserve the confidentiality of NORS filings. The Commission will grant access to NORS only after Participating Agencies certify that they will comply with requirements for maintaining the confidentiality of the data and the security of the databases. While Participating Agencies may share this information with local emergency management agencies that similarly have a "need to know," these "Downstream Agencies" are not themselves permitted direct access to NORS. Participating Agencies are responsible for ensuring Downstream Agencies certify that they, too, will maintain the confidentiality of the data they receive.

NORS Information Sharing users are provided read-only access to geographically applicable filings.

To apply for NORS and DIRS access, a complete application must be sent to NORS_DIRS_Information_Sharing@fcc.gov. This includes:

- a signed statement from an agency official, on the agency's official letterhead, including the official's full contact information and formally requesting access to NORS and DIRS filings;
- a description of why the agency has a need to access NORS and DIRS filings and how it intends to use the information in practice;
- if applicable, a request to exceed the proposed presumptive limits on the number of individuals (i.e., user accounts) permitted to access NORS and DIRS filings with an explanation of why this is necessary;
- a completed copy of a Participating Agency Certification Form; and

- a demonstration of the agency's "need to know" by citing to statutes or other regulatory authority that establishes it has official duties making it directly responsible for emergency management and first responder support functions.

The Participating Agency Certification Form and related materials can be found at: http://www.fcc.gov/outage-information-sharing

Once approved, an agency must create dedicated email accounts that it will use to access the system (a maximum of five), in order to allow the agency itself to manage the accounts in response to staff changes. The email addresses must be registered in the FCC's COmmission REgistration System (CORES), available at https://apps.fcc.gov/cores/userLogin.do. Once registered in CORES, an agency may request NORS and/or DIRS access for those the email addresses by logging into each database and requesting access. For NORS, see Section 3 of this manual. For DIRS, please refer to that manual's processes.

Participating Agencies are responsible for managing and maintaining the integrity of their accounts.

3. Accessing NORS

3.1. Locating NORS

To locate the NORS application,

Either go directly to the FCC NORS page (Figure 2) by inserting the following URL into a browser:

https://www.fcc.gov/network-outage-reporting-system-nors#block-menu-block-4

OR

1. Go to the FCC homepage (https://www.fcc.gov/).
2. Click on the ***Browse by Category*** menu located at the top of the page (Figure 1). Note: This menu allows users to view six separate drop-down menus.
3. Click on the ***Licensing & Database*** tab (Figure 1, red rectangle).
4. Click on the ***NORS*** link (Figure 1, red arrow).

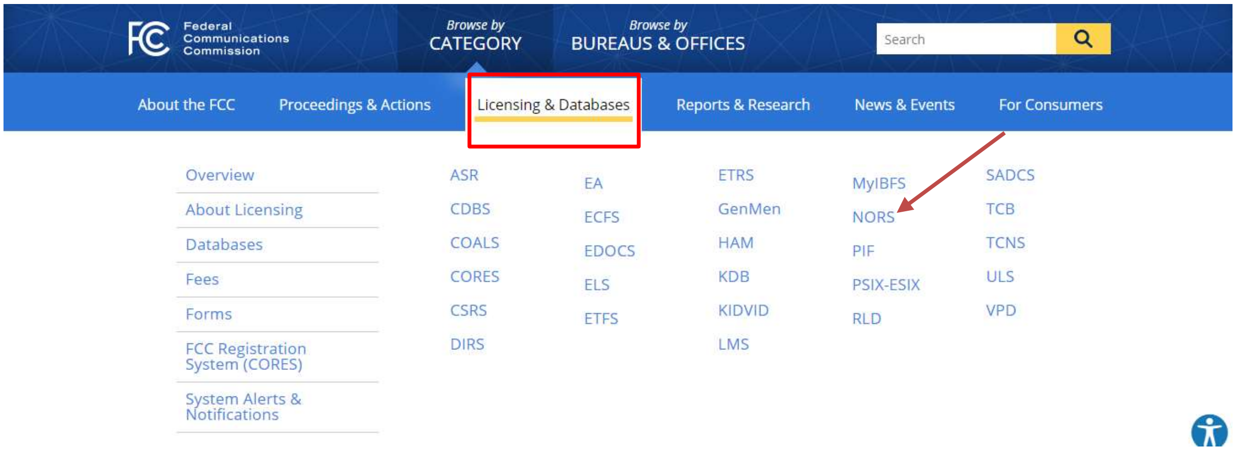
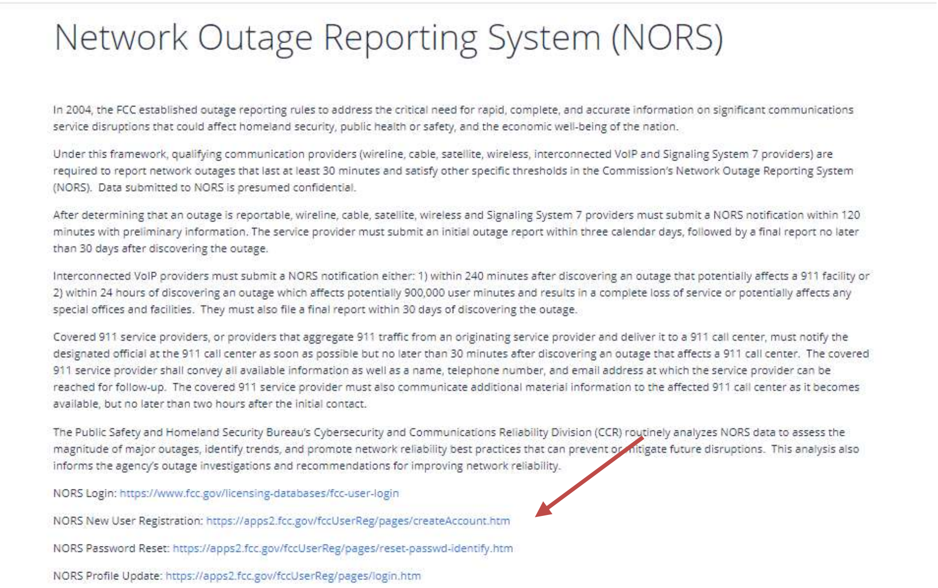


Figure 1. FCC Homepage > Browse by Category > Licensing & Database Menu > NORS

3.2. New Users

Selecting the FCC NORS link connects the user to the FCC NORS page. A user must create an account prior to gaining access to NORS. To create a new account, select the NORS New User Registration link shown in Figure 2.



Network Outage Reporting System (NORS)

In 2004, the FCC established outage reporting rules to address the critical need for rapid, complete, and accurate information on significant communications service disruptions that could affect homeland security, public health or safety, and the economic well-being of the nation.

Under this framework, qualifying communication providers (wireline, cable, satellite, wireless, interconnected VoIP and Signaling System 7 providers) are required to report network outages that last at least 30 minutes and satisfy other specific thresholds in the Commission's Network Outage Reporting System (NORS). Data submitted to NORS is presumed confidential.

After determining that an outage is reportable, wireline, cable, satellite, wireless and Signaling System 7 providers must submit a NORS notification within 120 minutes with preliminary information. The service provider must submit an initial outage report within three calendar days, followed by a final report no later than 30 days after discovering the outage.

Interconnected VoIP providers must submit a NORS notification either: 1) within 240 minutes after discovering an outage that potentially affects a 911 facility or 2) within 24 hours of discovering an outage which affects potentially 900,000 user minutes and results in a complete loss of service or potentially affects any special offices and facilities. They must also file a final report within 30 days of discovering the outage.

Covered 911 service providers, or providers that aggregate 911 traffic from an originating service provider and deliver it to a 911 call center, must notify the designated official at the 911 call center as soon as possible but no later than 30 minutes after discovering an outage that affects a 911 call center. The covered 911 service provider shall convey all available information as well as a name, telephone number, and email address at which the service provider can be reached for follow-up. The covered 911 service provider must also communicate additional material information to the affected 911 call center as it becomes available, but no later than two hours after the initial contact.

The Public Safety and Homeland Security Bureau's Cybersecurity and Communications Reliability Division (CCR) routinely analyzes NORS data to assess the magnitude of major outages, identify trends, and promote network reliability best practices that can prevent or mitigate future disruptions. This analysis also informs the agency's outage investigations and recommendations for improving network reliability.

NORS Login: https://www.fcc.gov/licensing-databases/fcc-user-login

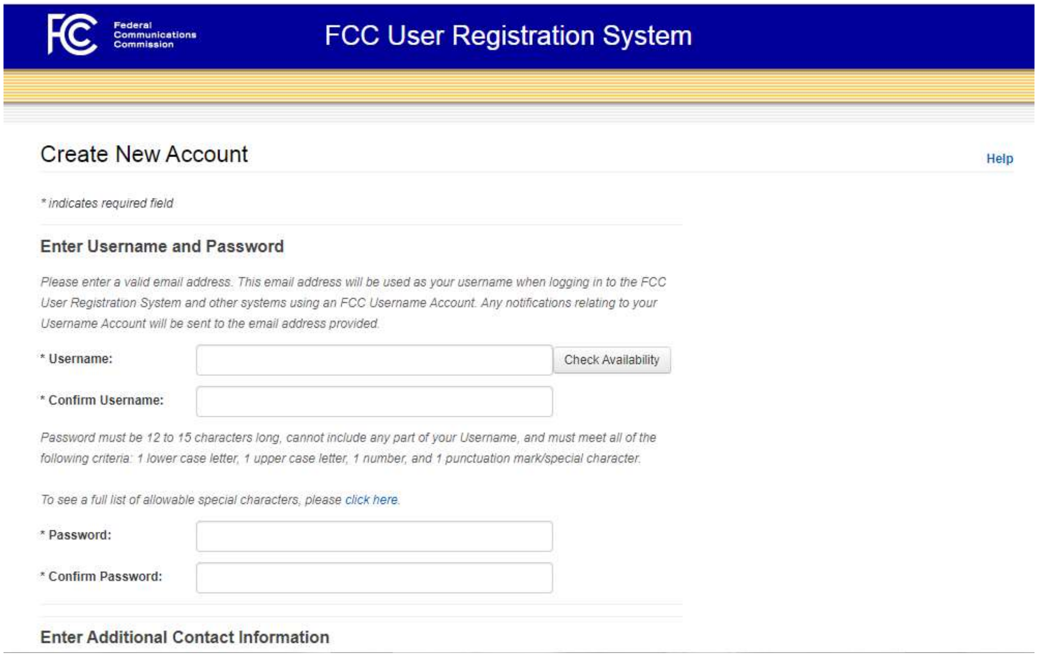
NORS New User Registration: https://apps2.fcc.gov/fccUserReg/pages/createAccount.htm

NORS Password Reset: https://apps2.fcc.gov/fccUserReg/pages/reset-passwd-identify.htm

NORS Profile Update: https://apps2.fcc.gov/fccUserReg/pages/login.htm

Figure 2. New User Registration link on FCC NORS page

This will provide the Create New Account page shown in Figure 3. This will create a Username Account for an individual in the FCC's Commission Registration System (CORES). The CORES login will allow access to a multitude of FCC systems. Users with a preexisting CORES account can use that account to access NORS.



FCC User Registration System

Create New Account

*indicates required field

Enter Username and Password

Please enter a valid email address. This email address will be used as your username when logging in to the FCC User Registration System and other systems using an FCC Username Account. Any notifications relating to your Username Account will be sent to the email address provided.

* Username:

* Confirm Username:

Password must be 12 to 15 characters long, cannot include any part of your Username, and must meet all of the following criteria: 1 lower case letter, 1 upper case letter, 1 number, and 1 punctuation mark/special character.

To see a full list of allowable special characters, please click here.

* Password:

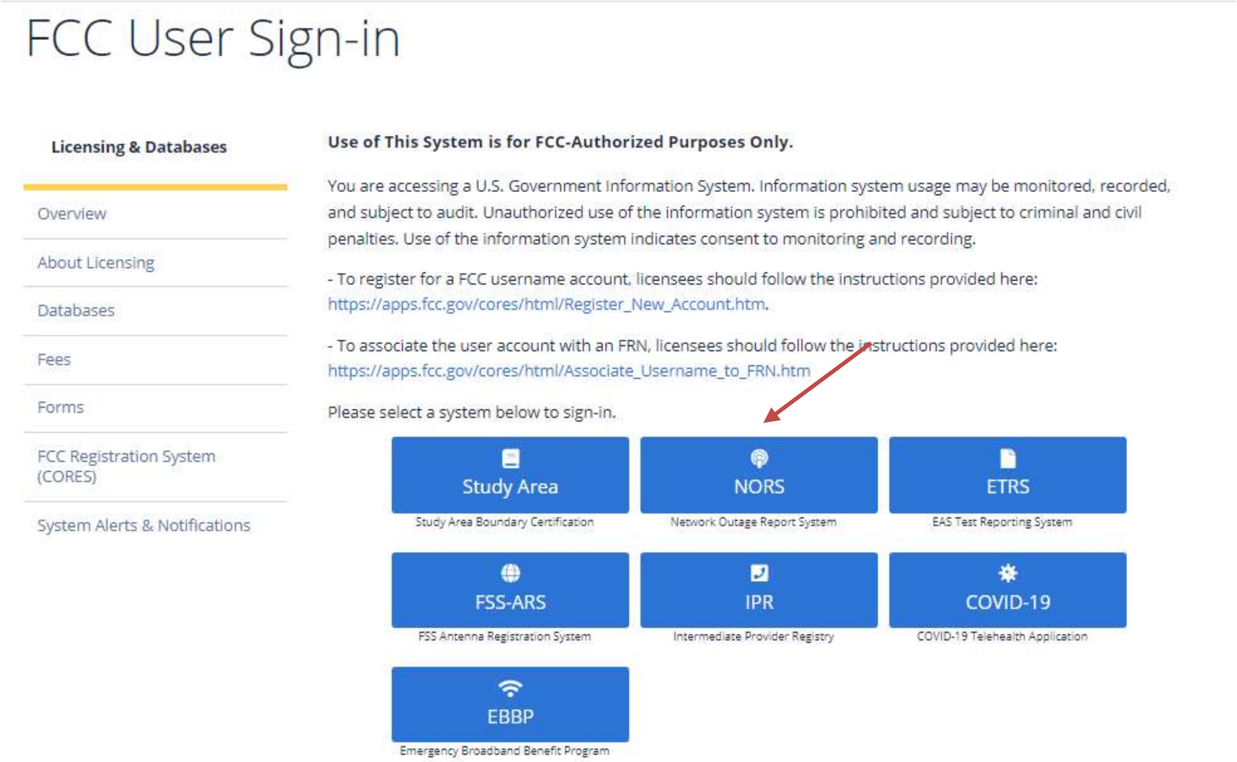
* Confirm Password:

Enter Additional Contact Information

Figure 3. Request New User Account

3.3. Logging in to NORS

Choosing the NORS login link found on the FCC NORS page will bring you the FCC sign in page shown in Figure 4.



FCC User Sign-in

Licensing & Databases

- Overview
- About Licensing
- Databases
- Fees
- Forms
- FCC Registration System (CORES)
- System Alerts & Notifications

Use of This System is for FCC-Authorized Purposes Only.

You are accessing a U.S. Government Information System. Information system usage may be monitored, recorded, and subject to audit. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties. Use of the information system indicates consent to monitoring and recording.

- To register for a FCC username account, licensees should follow the instructions provided here: https://apps.fcc.gov/cores/html/Register_New_Account.htm.

- To associate the user account with an FRN, licensees should follow the instructions provided here: https://apps.fcc.gov/cores/html/Associate_Username_to_FRN.htm

Please select a system below to sign-in.

Study Area
Study Area Boundary Certification
NORS
Network Outage Report System
ETRS
EAS Test Reporting System
FSS-ARS
FSS Antenna Registration System
IPR
Intermediate Provider Registry
COVID-19
COVID-19 Telehealth Application
EBBP
Emergency Broadband Benefit Program

Figure 4. FCC User Sign-in Screen

Click on the NORS icon as shown. The login screen will appear (Figure 5):

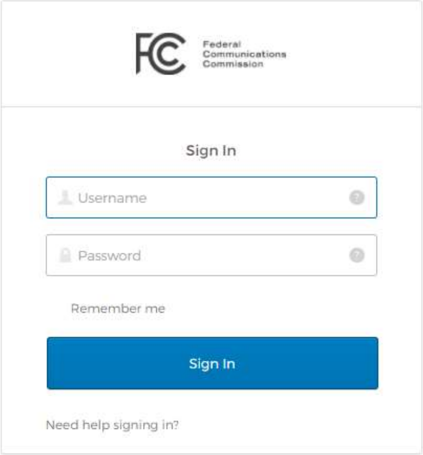


Figure 5. FCC Log-in Screen

The access page will display a Security Banner by which you acknowledge you are accessing a U.S. Government information system, and warning against unauthorized or improper use.

3.4. Requesting User Access

Prior to being able to see relevant NORS outages, Users must request access. Start by selecting the

Request to be Assigned as a Federal, State or Tribal User from the ServiceNow sidebar (Figure 6).

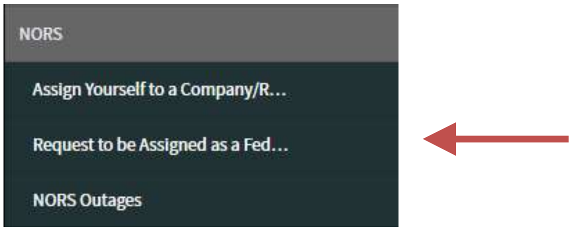
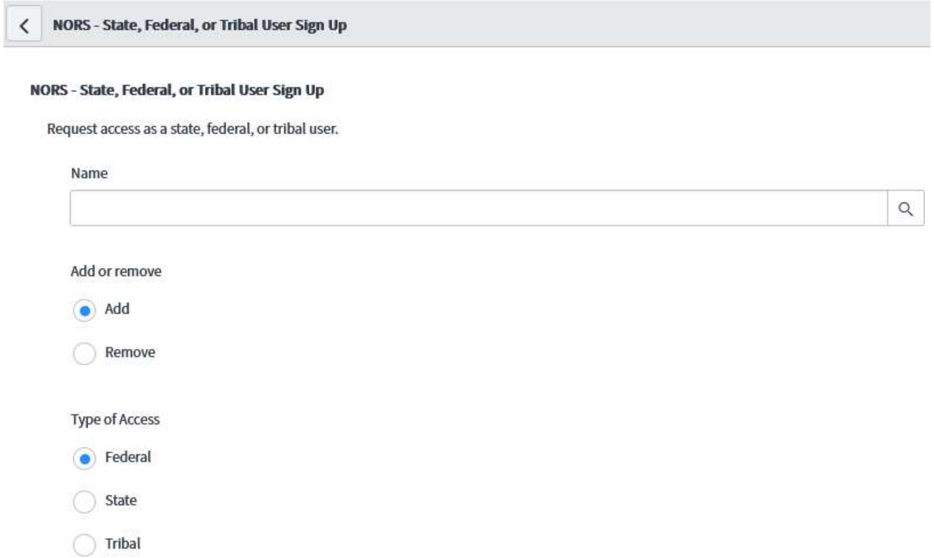

NORS
Assign Yourself to a Company/R...
Request to be Assigned as a Fed...
NORS Outages

Figure 6. NORS Sidebar Request to Be Assigned a User

This will show the screen found in Figure 7. Complete the displayed fields. After submission, the request will be reviewed by the NORS administrative team. Agencies can repeat this process to request access for up to five dedicated e-mail addresses. Once all requests are submitted, Agencies must then send an e-mail to FCC staff at NORS_DIRS_Information_Sharing@fcc.gov that lists the e-mail addresses for which they have requested access. FCC staff will validate the addresses and grant access. After your request is approved, NORS outages will populate in the NORS dashboard.



NORS - State, Federal, or Tribal User Sign Up

NORS - State, Federal, or Tribal User Sign Up

Request access as a state, federal, or tribal user.

Name

Add or remove

● Add

○ Remove

Type of Access

● Federal

○ State

○ Tribal

Figure 7. User Access Request Form

3.5.Reset Password

If you have forgotten your password or otherwise wish to change it, click on “Need help signing in?” in the lower left corner of the Log-in screen. The Log-in screen will change as shown in Figure 8.

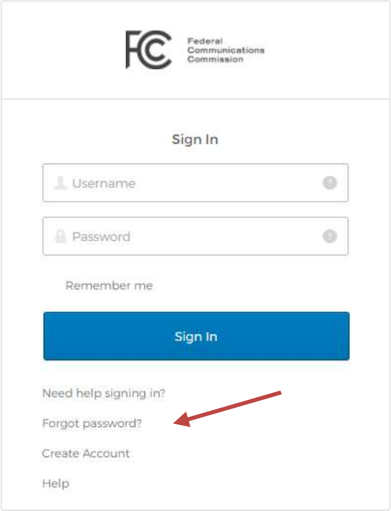
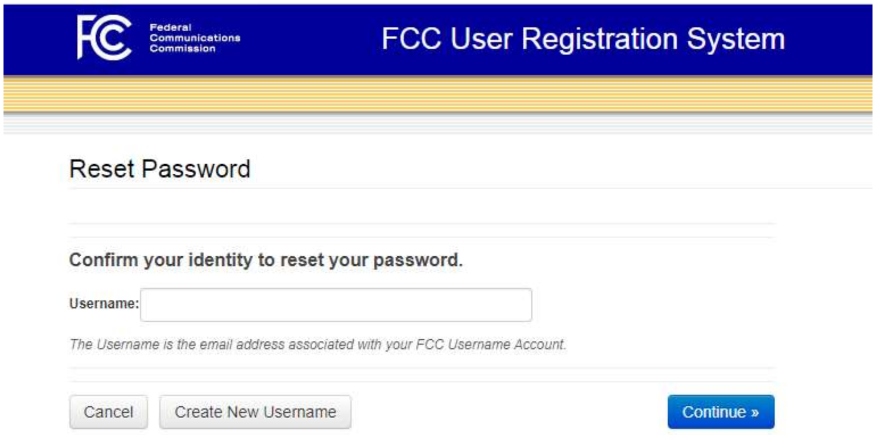


Figure 8. FCC Log-in Screen for Persons Needing Help Logging in

To change passwords, click on “Forgot password?” (Figure 8, red arrow). This will take you to the Reset Password screen (Figure 9):


Federal Communications Commission
FCC User Registration System

Reset Password

Confirm your identity to reset your password.

Username:

The Username is the email address associated with your FCC Username Account.

Cancel
Create New Username
Continue »

Figure 9. Reset Password

Enter the email address associated with your NORS account and press the “Continue” button. Then follow the instructions on the screen.

3.6. Updating Profile

To update your profile once logged in, click the username located in the top right-hand corner of the screen, and select the ***Profile*** link (Figure 10). You can then make changes to your name, business phone number, mobile phone number, position title, email address, preferred date format, and preferred time zone.

3.7. Logging Out

To log out of the ServiceNow system (i.e., end the session and log out), click the username located in the top right-hand corner of the screen, and select the ***Logout*** link (Figure 10).

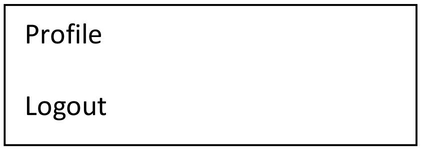


Figure 10. Changing Profile/Logging Out

4. NORS Outage Reports

Once logged in, select the NORS Outage tab from the sidebar, highlighted in Figure 11, to access the NORS dashboard.

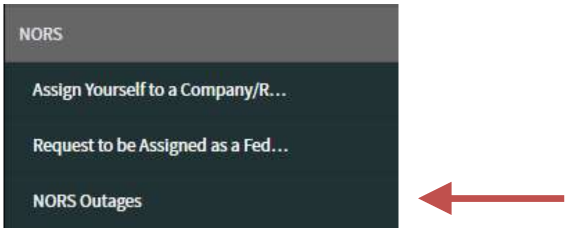
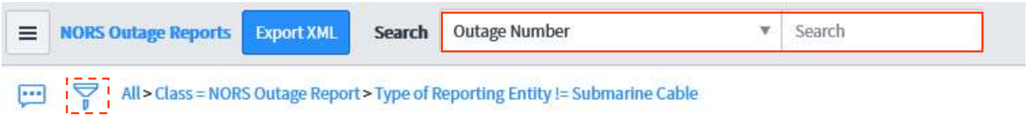

NORS
Assign Yourself to a Company/R...
Request to be Assigned as a Fed...
NORS Outages

Figure 11. NORS Sidebar tab for NORS Outages

4.1.Searching NORS

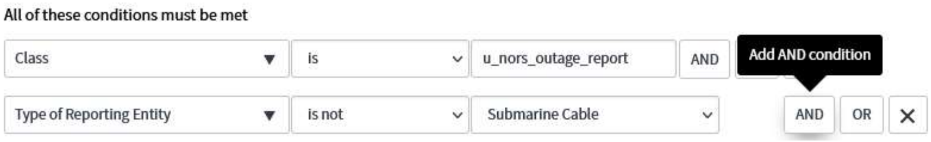
By default, the NORS dashboard will show the 20 most recent outage updates. NORS has the ability to filter outages based on certain criteria or a specific outage by entering the outage number. Figure 12 highlights the outage number search bar in solid red and the NORS filter icon in a dashed red line.



All > Class = NORS Outage Report > Type of Reporting Entity != Submarine Cable

Figure 12. NORS Filter Icon and Outage Number Search Bar

Selecting the NORS filter icon will open the search conditions menu. By default, the dashboard includes the searchable conditions for a NORS outage report and does not include submarine cable outages. NORS outages are filtered by adding additional conditions to these search defaults. Selecting the AND icon (as shown in Figure 13) will open an additional condition line.

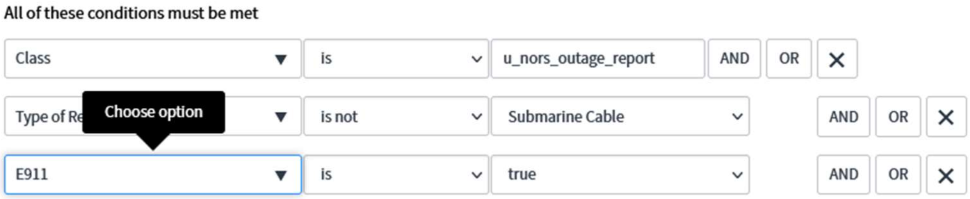

All of these conditions must be met

Class ▼ | is | u_nors_outage_report | AND

Type of Reporting Entity ▼ | is not | Submarine Cable

Figure 13. NORS Search Conditions

The additional condition line includes a condition option, an operator and a second option based on the operator. The *Glossary of Fields in NORS Reports* (Appendix A) provides a list and definitions of all the available search condition options. Figure 14 shows the condition option of E911.

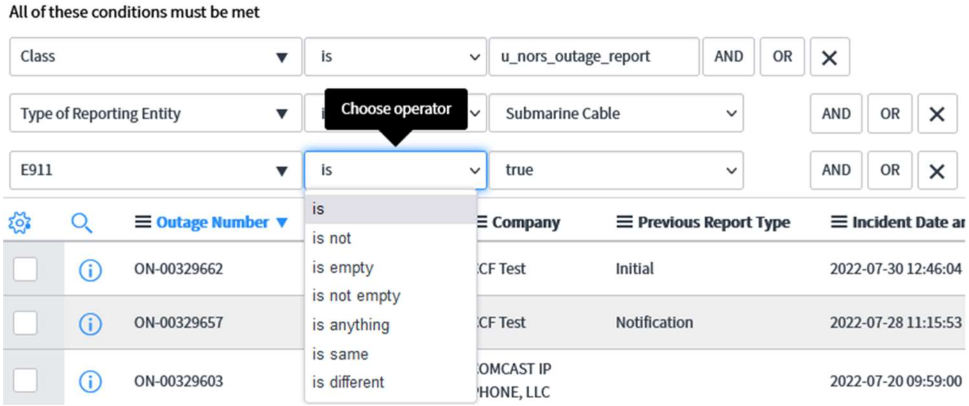


All of these conditions must be met

Class ▼	is	u_nors_outage_report	AND	OR	✕
Type of Re ▼	is not	Submarine Cable	AND	OR	✕
E911 ▼	is	true	AND	OR	✕

Figure 14. E911 NORS Outage Report Condition Option

Figure 15 shows the available condition operators available when searching for E911 outages. The condition operators change based on the search option.



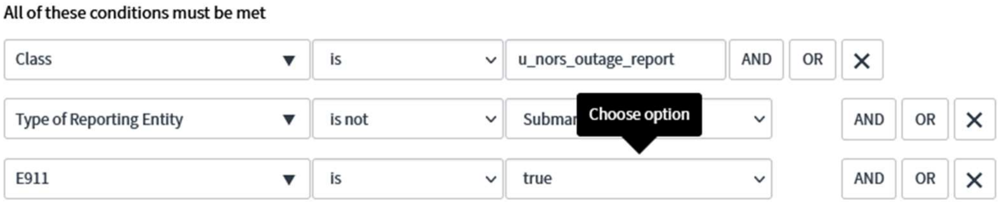
All of these conditions must be met

Class ▼	is	u_nors_outage_report	AND	OR	✕
Type of Reporting Entity ▼	i	Submarine Cable	AND	OR	✕
E911 ▼	is	true	AND	OR	✕

Outage Number ▼	Company	Previous Report Type	Incident Date ar
ON-00329662	CF Test	Initial	2022-07-30 12:46:04
ON-00329657	CF Test	Notification	2022-07-28 11:15:53
ON-00329603	OMCAST IP HONE, LLC		2022-07-20 09:59:00

Figure 15: E911 Operator for NORS Outage Report Conditions

Figure 16 shows the final condition option which applies to the operator. In this case the search criteria will provide a NORS Report, that is not a submarine cable outage and had an effect on E911 services.

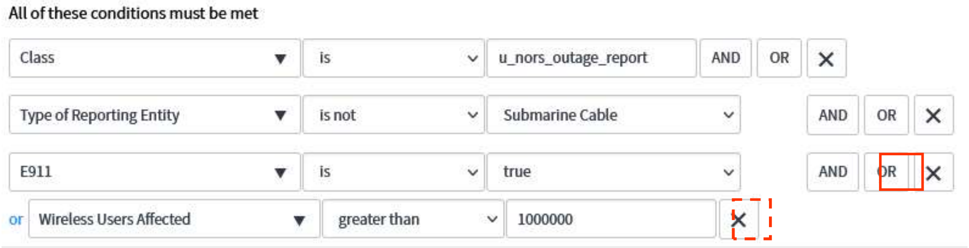


All of these conditions must be met

Class ▼	is	u_nors_outage_report	AND	OR	✕
Type of Reporting Entity ▼	is not	Submar	AND	OR	✕
E911 ▼	is	true	AND	OR	✕

Figure 16. E911 Operator Based Condition for NORS Outage Report Searches

After the first additional search condition is added, further conditions can be applied using the AND and OR buttons to the right. Selecting AND will create a condition that must be met in addition to the E911 criteria that was shown in Figure 16. Using the OR operator (highlighted in red in Figure 17) will create a condition which will show all NORS outages which meet at least one of the two added conditions. To remove a condition, select the X button highlighted in red dashed in Figure 17.



All of these conditions must be met

Class ▼ is u_nors_outage_report

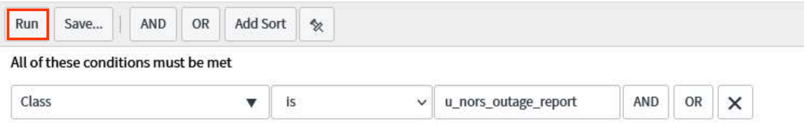
Type of Reporting Entity ▼ is not Submarine Cable

E911 ▼ is true

or Wireless Users Affected ▼ greater than 1000000

Figure 17: NORS Report Search Conditions Using the OR Operator

Once the search conditions are completed select Run (highlighted in Figure 18)



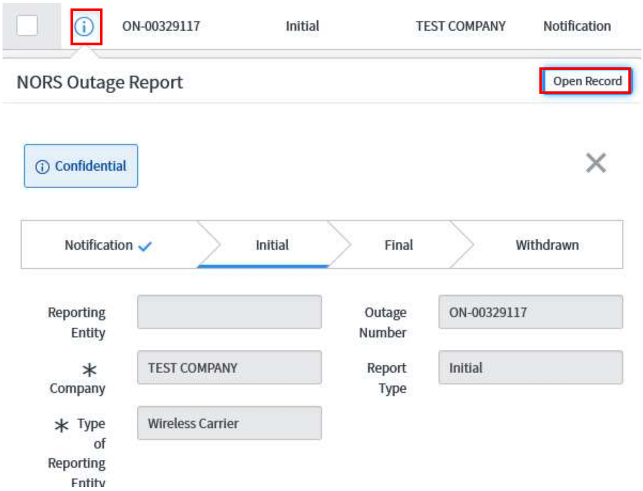
All of these conditions must be met

Class ▼ is u_nors_outage_report

Figure 18. Run the NORS Outage Conditions

4.2.NORS Outage Reports

To open a NORS Outage Report first click on the information icon show in Figure 19. This will open a preview tab of the outage. To gain access to the full outage report, click on Open Record. The explanation of the NORS report fields can be found in the *Glossary of Fields in NORS Reports* (Appendix A).



ON-00329117 Initial TEST COMPANY Notification

NORS Outage Report

Reporting Entity:

Outage Number: ON-00329117

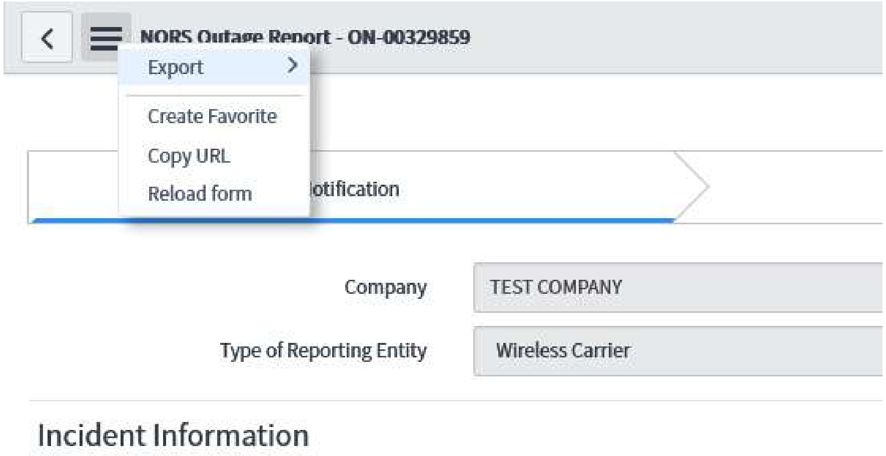
∗ Company: TEST COMPANY

Report Type: Initial

∗ Type of Reporting Entity: Wireless Carrier

Figure 19. Opening a NORS Outage Report

Opening the NORS outage record will allow access to the export menu found in the top left corner as shown in Figure 20.   Exported NORS outages remain confidential.



Company: TEST COMPANY

Type of Reporting Entity: Wireless Carrier

Figure 20. Exporting a NORS Outage Report

5. Submarine Cable Outages (Applicable to Federal Users)

Federal users will have access to Submarine Cable Outages. To access Submarine Cable outages, select SC NORS Outages from the ServiceNow sidebar.

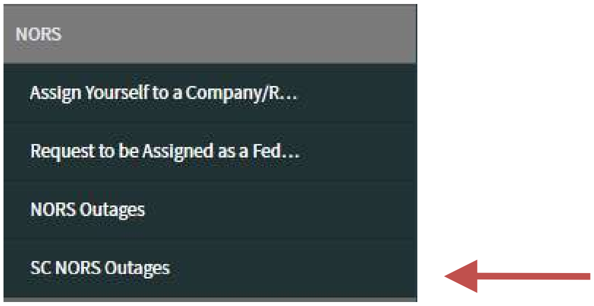
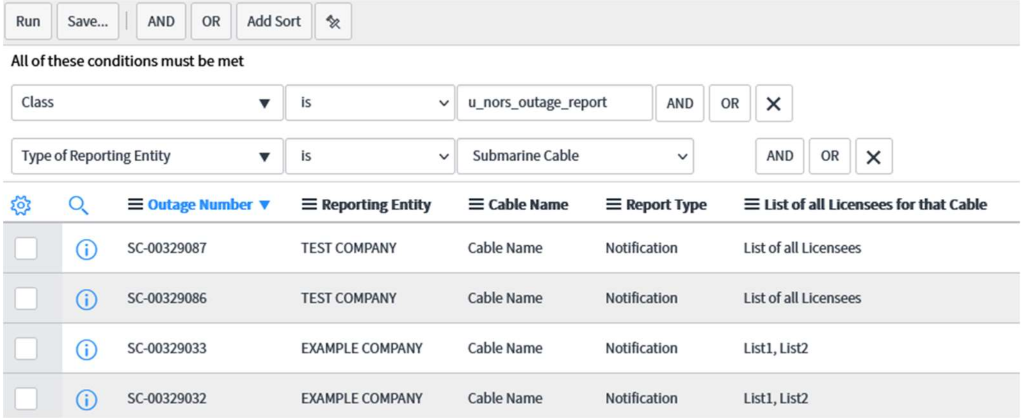

NORS
Assign Yourself to a Company/R...
Request to be Assigned as a Fed...
NORS Outages
SC NORS Outages

Figure 21. NORS Sidebar SC NORS Outages

Figure 22 shows an example of the Submarine Cable NORS outage dashboard. Submarine Cable outages have outage numbers that start with SC. Searching for Submarine Cable outages is done in the same manner as searching for NORS outages.



All of these conditions must be met

Class ▼ is u_nors_outage_report AND OR ✕

Type of Reporting Entity ▼ is Submarine Cable AND OR ✕

		Outage Number ▼	Reporting Entity	Cable Name	Report Type	List of all Licensees for that Cable
□	ⓘ	SC-00329087	TEST COMPANY	Cable Name	Notification	List of all Licensees
□	ⓘ	SC-00329086	TEST COMPANY	Cable Name	Notification	List of all Licensees
□	ⓘ	SC-00329033	EXAMPLE COMPANY	Cable Name	Notification	List1, List2
□	ⓘ	SC-00329032	EXAMPLE COMPANY	Cable Name	Notification	List1, List2

Figure 22. Submarine Cable Example Dashboard

Appendix A

FEDERAL COMMUNICATIONS COMMISSION · USA ·

Network Outage Reporting System

Glossary of Fields in NORS Reports

Version 2

Section 1 - Fields on the Initial and Final Report Forms for Outages Other than Submarine Cable Outages

Note that all of the data previously filled in are carried forward when updating a report. All fields can be changed by communications providers to reflect new information except the Outage Number and Company.

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

Updated At time: Updated at date-times are generated automatically by NORS. They do not appear on the report input forms, but they are displayed at the bottom of the record or report for an individual outage.

Report Type –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 the Initial report.

Company – Lists the name of the company filing the outage report, which is automatically filled in from the Notification. Outage reports must be filed with the FCC by any cable communications provider, wireless service provider, satellite operator, SS7 provider, wireline communications provider, paging provider, E911 service provider, or facility owner and on any facilities which it owns, operates or leases that experiences an outage that meets the reporting thresholds as defined in Part 4 of the Commission's rules.

Type of Reporting Entity – Lists company type. This entry is automatically filled with the information taken from the Notification, but can be changed. The possible entries are:

Wireline Carrier
Wireless Carrier
Cable telephony provider
Paging provider
Satellite provider
SS7 network provider
E911 service provider
Facility owner or operator
VoIP provider

Incident Date and Time - Provides the month, day and year at the commencement of the outage. See also the discussion of **Time Zone** below.

Date and Time Determined Reportable - Date and time at which a company determines that an outage has occurred and meets one or more of the reportable thresholds. See also the discussion of **Time Zone** below.

Time Zone – Communications providers pick one of the following from the scroll down menu:

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

Puerto Rico and the Virgin Islands are both in the Atlantic time zone. “Other” should be used for other territories, such as American Samoa.

Reason Reportable – Provides the threshold that was crossed to determine that this outage was reportable. If more than one threshold was crossed, please choose the primary reason. Communications providers pick one of the following from the scroll down menu:

Wireline – 900,000 user-minutes
Wireless – 900,000 user-minutes
Cable telephony – 900,000 user-minutes
MSC
E911
Blocked Calls
667 OC3 minutes
OC3-Simplex greater than 4 Days (not shared with Participating Agencies)
SS7 - MTP Messages
Airport
Other Special Facilities - (Military, nuclear, etc.)
Paging
Satellite
Other
VoIP – E911
VoIP – 900,000 user-minutes

Outage Duration - Provides the total elapsed time (hours and minutes) from the commencement of the outage as provided in the preceding data fields until restoration of fu1l service. For example, if the outage duration is 10 hours and 42 minutes, communications providers place 10 in the Outage Duration (Hours) field and 42 in the Outage Duration (Minutes) field.

Full service restoration includes the restoration of all services to all customers impacted by the outage, even if the restoral is over temporary facilities. If the customers' locations are destroyed such as by a hurricane, flood, tornado, or wildfire, the duration continues until the reporting carrier is capable of again providing service to those locations. If an outage is ongoing at the time the Final report is filed, communications providers report the outage duration hours as"9999" and indicate in the description that the outage was ongoing at the time the final report is submitted.

Explanation of Outage Duration (for incidents with partial restoration times) – Describes 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, communications providers provide information on the number of users in each block restored to service and the elapsed time to partial restoration 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. For outages that last an unusually long time, communications providers should provide an explanation in this field.

Inside Building Indicator – Selects "Yes" if the outage occurred inside a building owned, leased, or otherwise controlled by the reporting entity**.** Otherwise**,** selects "No."

E911 Outage– For non-E911 outages, selects "E911 Not Affected" from the scroll down menu. For E911 outages, selects one of the following from the scroll down menu:

ALI Only Affected – For wireline carriers, when location of the caller could not be provided but the call could be routed to a PSAP.
Phase II Only Affected – For wireless outages, when Phase II location information could not be provided but the call could be routed to a PSAP.
Phase I and Phase II Only Affected – For wireless outages, when neither Phase I nor Phase II 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 in Other Company- Checks "Yes" if the failure occurred in another company's network. Otherwise, checks "No".

Services Affected

Cable Telephone – Checks the box if cable telephony users were affected.
Wireless (not paging) - Checks the box if wireless users were affected.
VoIP - Checks the box if VoIP users were affected.
E911 - Checks the box if E911 service or some aspect of E911 service was affected.
Paging - Checks the box if paging users were affected by the outage.

Satellite - Checks the box if satellite facilities were affected by the outage.
Signaling (SS7) - Checks the box if SS7 service was affected by the outage.
Wireline - Checks the box if wireline users were affected by the outage. This includes outages where only intraLATA service or only interLATA service was affected.
Special Facilities - Checks the box if any service enrolled in the Telecommunications Service Priority (TSP) Program at priority Levels 1 and/or 2 lost telecommunication service.
Other Service

Number of Potentially Affected

Wireline Users Affected – Provides 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, field is left 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 Affected – Provides the number of potentially affected wireless users. If this outage did not affect wireless users, please leave this blank.

VoIP Users Affected – Provides the number of potentially affected VoIP users. If this outage did not affect VoIP users, please leave this blank.

Paging Users Affected - Provides 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, field is left blank.

Cable Telephone Users Affected - Provides the number of assigned telephone numbers. If this outage did not affect cable telephony users, field is left blank.

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

Number of Affected OC3s – Provides the number of previously operating OC3s that were affected by the outage and were out of service for 30 or more minutes, regardless of the services carried on the OC3s or the utilization of the OC3s.

OC3s restored to service in fewer than 30 minutes should not be included in the count of the number of OC3s affected. For example, if an outage initially took 192 OC3s out of service, but 128 were restored to service in less than 30 minutes, then only 64 were out of service for 30 minutes or longer; consequently, the number of affected OC3s should be recorded as “64”.

If some failed OC3s were initially knocked out of service but restored in fewer than 30 minutes, the rapid restoration of those OC3s can be noted in the “Description of Incident” field, but they should not be included in the count of the number of OC3s affected.

Communications providers should count any failed STS3c as a failed OC3, a failed STS12c as 4 OC3s, etc.

Number of Blocked Calls – Provides the number of blocked calls.

If no calls were blocked, communications providers should leave the field blank or enter “0”.

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.

Blocked Calls Realtime and Blocked Calls Historic – If the number of Blocked Calls is provided, communications providers check whether this number came from real-time data or was based on historic carried loads the same day(s) of the week and the same time(s) of day as the outage.

Number of Lost SS7 MTP Messages - In cases of an SS7 outage and where an SS7 provider cannot directly estimate the number of blocked calls, provides 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 historic information should not be older than 90 days preceding the onset of the outage. If the outage does not affect an SS7 network, field is left blank.

Lost SS7 Messages Realtime and Lost SS7 Messages Historic –If the Number of Lost SS7 MTP Messages is provided, communications provider checks whether this number came from real-time data or was based on historic carried traffic the same day(s) of the week and the same time(s) of day as the outage.

Mobile Switching Center (MSC) Failed – Checks "Yes" if the outage included an MSC failure. Checks "No" if the outage did not include an MSC failure. Checks "N/A" if your network does not have MSCs.

Geographic Area Affected

State Affected – Chooses the state(s) affected by the outage from the scroll down menu. All 50 states along with the District of Columbia, Virgin Islands, Puerto Rico, and Guam are listed. Outages occurring outside the 50 states, the District of Columbia, Virgin Islands, Puerto Rico, or Guam are listed as "OTHER: OUTSIDE 50 STATE." Entering a letter in the field will highlight the first state starting with that letter in the list.

City Affected – Provides the (primary) city affected.

Description of Incident - Provides 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.

Description of the Cause(s) of the Outage – Provides a text description of all the causes of the outage.

Direct Cause: The direct cause is the immediate event that results in an outage – The direct cause is the event, action, or procedure that triggered the outage. Section 5 provides 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 –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. Section 5 provides a complete description of each root cause. For example, a cable cut from improper marking could be the triggering event or direct cause but the real cause (root cause) may be lack of diversity.

Contributing Factors –Contributing factors are problems or causes that are closely linked to the outage. Often if a contributing factor had been 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 5.

Lack of Diversity– Communications providers check "Yes" if lack of diversity contributed to or caused the outage. Otherwise, communications providers check "No." 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, communications providers must determine whether engineering standards for diversity are being followed.

Malicious Activity – Indicates whether the communications provider believes that malicious activity might be involved in the outage.

If yes - please explain Malicious Activity – Provides an explanation of why the communications provider believes the activity is malicious or what is suspicious about the activity if "Yes - Cyber" or "Yes - Physical" is selected in the Malicious Activity field.

Name and Type of Failed Equipment - Provides 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 Network Involved – Provides 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 - Provides a complete, chronological narrative of the methods used to restore service, both "quick fix" and final.

Was Telecommunications Service Priority Involved in Service Restoration? – Communications provider checks "Yes" if TSP was involved during service restoration. Otherwise, communications provider checks "No."

Steps Taken to Prevent Recurrence – Provides 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 – Provides 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. The Best Practices can also be accessed by clicking on "Click here" under "To view the NORS Best Practice Page:" in the Help Center section of the NORS Homepage.

Best Practices used to mitigate effects of Outage - Provides 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, field is left blank. Best Practices can be sourced from the https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm or http://www.atis.org/bestpractices. The Best Practices can also be accessed by clicking on "Click here" under "To view the NORS Best Practice Page:" in the Help Center section of the NORS Homepage.

Analysis of Best Practice – Provides 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, communications provider shouldindicate.

Remarks – Provide any additional information that the service provider believes is relevant, but did not fit anyplace else on the form.

Primary Contact

Primary Contact information is prepopulated with information from the latest report. Alternatively, the information can be provided manually in each field.

Name – 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 or NPANXXXXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Extension – Provide an extension number if needed.

U.S. Postal Service Address – Optional. May provide the address of the primary contact person using the fields Address Line 1, Address Line 2, and Address Line 3.

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

Section 2 - Fields on the Notification Form for a Submarine Cable Outage

Reporting Entity – This gives the name of the reporting entity filing the outage report. The Commission requires submarine cable licensees to submit outage reports regarding disruptions to communication when disruptions meet the reporting thresholds as defined in Section 4.15 of the Commission's Rules. For cables with multiple licensees, the licensees may jointly designate a single "responsible licensee", and that licensee would become the "reporting entity" for outages of the affected submarine cable. For a cable with only one licensee, that licensee would be the "reporting entity" for NORS purposes.

Type of Reporting Entity – For a submarine cable outage report, the type of reporting entity will always be Submarine Cable Reporting Entity.

Cable Name – As given in the license.

List of All Licensees for that Cable – As given in the license.

Incident Date and Time - Provides the date and time of the commencement of the outage.

Time Zone – In a submarine cable outage report, all times should be entered as Greenwich Mean Time (GMT).

Date and Time Determined Reportable - Date and time at which a company determines that an outage has occurred and meets one or more of the reportable thresholds.

Description of Event - Provides 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.

Description of Causes– Provides a text description of all the causes of the outage.

Was Event Related to Planned Maintenance? – Indicates whether the event resulted directly or indirectly from planned maintenance.

Location of Cable Landing Station Closest to Failure Site – Provides the country (Country of Cable Landing Station Closest to Failure Site) and city (City of Cable Landing Station Closest to Failure Site) in which the cable landing closest to the point of failure is located.

Location of the Event – Provides the location of the cable break or other failed unit. There are two formats in which this information may be provided.

Miles and Direction

Miles – Provides the distance in nautical miles from the nearest landing.

Direction – Provides the direction of the failure site relative to the nearest landing. For example, if the break is located northwest of the nearest landing, enter "northwest" in this field.

Latitude and Longitude

Latitude – Provides the latitude of the point of failure. This should be specified in degrees and fractions of a degree, rather than degrees, minutes, seconds, and fractions of a second. This number should be followed by N or S, depending on whether it is a location North or South of the equator. The number should be accurate to one hundredth of a degree.

Longitude – Provides the longitude of the point of failure. This should be specified in degrees and fractions of a degree, rather than degrees, minutes, seconds, and fractions of a second. This number should be followed by E or W, depending on whether it is a location East of West of the Greenwich Meridian. The number should be accurate to one hundredth of a degree.

Contact Information

Contact information is prepopulated with information from the profile of the person entering the information. Alternatively, the information in each field can be provided manually.

Contact Name – Provides the full name of the primary contact person.

Contact Email Address - Provides the e-mail address of the contact person

Contact Telephone Number – Provides the phone number of the primary contact person in the format NXX-NXX-XXXX or NPANXXXXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Section 3 - Fields on the Interim and Final Report Forms for Submarine Cable Outages

Note that all of the data previously filled in are carried forward when updating a report. All fields can be changed by communications providers to reflect new information except the Outage Number and Company.

Reporting Entity – Gives the name of the reporting entity filing the outage report, which is automatically filled in from the Notification. Submarine cable outage reports must be filed with the FCC by the cable licensee for any cable that experiences an outage that meets the reporting thresholds as defined in Section 4.15 of the Commission's Rules and Regulations. For cables with multiple licensees, the licensees may jointly designate a single “responsible licensee”, and that licensee would become the “reporting entity” for outages of the affected submarine cable.

Type of Reporting Entity– For a submarine cable outage report, the type of reporting entity will always be Submarine Cable Reporting Entity.

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

Report Type –The Interim report shall contain all available pertinent information on the outage, including at a minimum information for all mandatory fields in the report template, and shall be submitted in good faith. The Final report shall contain all pertinent information on the outage, including at a minimum information for all mandatory fields in the report template, and including any information that was not contained in or that has changed from the Interim report.

Cable Name – As given in the license.

List of All Licensees for that Cable – As given in the license.

Incident Date and Time - Provides the month, day and year at the commencement of the outage.

Date and Time Determined Reportable - Date and time at which a company determines that an outage has occurred and meets one or more of the reportable thresholds.

Time Zone – In a submarine cable outage report, all times should be entered as Greenwich Mean Time (GMT).

Outage Duration - Provides the total elapsed time (days and hours) from the commencement of the outage as provided in the preceding data fields until restoration of fu1l service. For example, if the outage duration is 10 days and 22 hours, place 10 in the Outage Duration (Days) field and 22 in the Outage Duration (Hours) field.

Full service restoration includes the restoration of all services to all customers impacted by the outage, even if the restoral is over temporary facilities. If the customers’ locations are destroyed such as by a hurricane, flood, tornado, or wildfire, the duration continues until the reporting carrier is capable of again providing service to those locations. If an outage is ongoing at the time the Final report is filed, communications providers report the outage duration hours as"9999" and also indicate in the description that the outage was ongoing at the time the final is submitted.

Description of Event - Provides 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.

Description of Causes – Provides a text description of all the causes of the outage.

Was Event Related to Planned Maintenance? – Indicates whether the event resulted directly or indirectly from planned maintenance.

Location of Cable Landing Station Closest to Failure Site – Provides the country (Country of Cable Landing Station Closest to Failure Site) and city (City of Cable Landing Station Closest to Failure Site) in which the cable landing closest to the point of failure is located.

Location of the Event – Provides the location of the cable break or other failed unit. There are two formats in which this information may be provided.

Miles and Direction

Miles – Provides the distance in nautical miles from the nearest landing.

Direction – Provide sthe direction of the failure site relative to the nearest landing. For example, if the break is located northwest of the nearest landing, enter "northwest" in this field.

Latitude and Longitude

Latitude – Provides the latitude of the point of failure. This should be specified in degrees and fractions of a degree, rather than degrees, minutes, seconds, and fractions of a second. This number should be followed by N or S, depending on whether it is a location North or South of the equator. The number should be accurate to one hundredth of a degree.

Longitude – Provides the longitude of the point of failure. This should be specified in degrees and fractions of a degree, rather than degrees, minutes, seconds, and fractions of a second. This number should be followed by E or W, depending on whether it is a location East of West of the Greenwich Meridian. The number should be accurate to one hundredth of a degree.

Date and Time when Plan of Work was Received
Estimate of when the Cable is Scheduled to be Repaired
Arrival Date and Time of Repair ship, if any
Date and Time of Repair

If any of the fields (except Date and Time of Repair) is not applicable, filer can enter N/A which will be changed to 0001-01-01 00:00:00 to indicate the field is not applicable.

Restoration method - Provides a complete, chronological narrative of the methods used to restore service, both "quick fix" and final.

Steps Taken to Prevent Recurrence – Provides 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.

Remarks – Provides any additional information that the communications provider believes is relevant, but did not fit anyplace else on the form.

Contact Information

Contact information is prepopulated with information from the profile of the person entering the information. Alternatively, the information in each field can be provided manually.

Contact Name – Provides the full name of the primary contact person.

Contact Email Address - Provides the e-mail address of the contact person

Contact Telephone Number – Provides the phone number of the primary contact person in the format NXX-NXX-XXXX or NPANXXXXXX. That is, 201-444-5656 would mean that the area code or NPA is 201, the central office code is 444, and the line number is 5656.

Updated At time: Updated at date-times are generated automatically by NORS. They do not appear on the report input forms, but they are displayed at the bottom of the record or report for an individual outage.

Section 4 - Fields on the Withdraw Report Dialog Box

Outage Number– This field is the unique identifying number for the report. It is automatically provided from the latest report submission.

Company or Reporting Entity Name – The name of the company or reporting entity filing the outage report, which is automatically provided from the latest report submission.

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

Section 5 - Descriptions of Root Cause, Direct Cause and Contributing Factors for Outages Other than Submarine Cable Outages

Cable Damage

Cable Unlocated

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

Digging Error

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

Inaccurate/ Incomplete Cable Locate

The cable's presence was determined, but its location was inaccurately and/or partially identified.

Inadequate/No Notification

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

Other

Shallow Cable

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

Cable Damage/Malfunction

Aerial/Non-Buried

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

Cable Malfunction

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

Design - Firmware

Ineffective Fault Recovery or Re-Initialization Action

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

Insufficient Software State Indications

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

Other

Design - Hardware

Inadequate Grounding Strategy

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

Other

Poor Backplane or Pin Arrangement

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

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

Mechanical/physical design problems.

Design – Software

Faulty Software Load - Office Data

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

Faulty Software Load - Program Data

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

Inadequate Defensive Checks

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

Ineffective Fault Recovery or Re-initialization Action

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

Other

Diversity Failure

External

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

Internal (Other)

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

Links

SS7 communication paths were not physically and logically diverse.

Power

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

Timing Equipment

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

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

Animal Damage

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

Earthquake

Component destruction or fault associated directly or indirectly with seismic shock. However, if damage was the result of inadequate earthquake bracing, consider the root cause to be Design - Hardware.

Fire

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

Flood

Ice/Storm

Lightning/Transient Voltage

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

Other

Storm - Water/Ice

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

Storm - Wind/Trees

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

Vandalism/Theft

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

Vehicular Accident

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

Environment (Internal)

Cable Pressurization Failure

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

Dirt, Dust Contamination

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

Environmental System Failure (heat/humidity)

Component loss or fault associated with extreme temperature, rapid temperature changes, or high humidity due to loss/malfunction of environmental control(s). If the failure was the result of inadequate/lack of response to (alarmed/un-alarmed) environmental failures, or due to incorrect manual control of environmental systems, consider the root cause to be a Procedural failure.

Fire Suppression (water, chemicals) Damage

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

Fire, Arcing, Smoke Damage

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

Manhole/Cable Vault Leak

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

Other

Roof/Air Conditioning Leak

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

Hardware Failure

Circuit Pack/Card Failure-Other

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

Circuit Pack/Card Failure-Processor

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

Memory Unit Failure

Other

Passive Devices

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

Peripheral Unit Failure

Processor Community Failure

Self-contained Device Failure

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

Shelf/Slot Failure

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

Software Storage Media Failure

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

Insufficient Data

Insufficient Data (no additional modifier)

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

Cleared While Testing

Service restored before the cause could be determined.

Non-Service Provider Personnel

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

Outside Owned Network

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

Under Investigation

Root cause analysis pending.

Other/Unknown

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Excludes cases where outage data were insufficient or missing, or where root cause is still under investigation. When root cause cannot be proven, it is usually still possible to determine the probable cause, which falls under the heading "Unknown." When classifications provided do not match the cause, the approximate match is preferred to be "Other."

Planned Maintenance

To Upgrade the System

Outage occurred during scheduled maintenance to upgrade the system or network element. The system or network element upgrade was completed successfully within expected times; however, FCC outage reporting thresholds were met.

To Fix Known Problems

Outage occurred during scheduled maintenance to fix known problems. The known problems were resolved successfully; however, FCC outage reporting thresholds were met.

Failed

Unexpected condition caused the planned maintenance activity to fail and FCC outage reporting thresholds were met.

Went Longer or Was Worse than Expected

The planned maintenance activity was completed successfully; however, due to unexpected conditions, planned maintenance took longer or had a greater impact than expected.

Power Failure (Commercial and/or Back-up) (does not include failures of DC/DC converters or fuses embedded in switches and transmission equipment, which should be reported as a Hardware Failure, unless the problem was caused by the power plant.)

Battery Failure

Batteries did not function as designed.

Breaker Tripped/Blown Fuses

Equipment failure associated with tripped breaker or blown fuse.

Extended Commercial Power Failure

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

Generator Failure
Generator did not function as designed or ran out of fuel.
Inadequate Site-Specific Power Contingency Plans
System failure due to the insufficiency of the emergency operating procedures and contingency plans available and the resulting outage is prolonged because of lack of site-specific information. This includes equipment engineering data, portable engine hook-up hardware/procedures, load shedding plans, etc.
Inadequate Back-up Power Equipment Located on Customer Premise
Customer premise power equipment unable to support communications equipment due to extended loss of commercial or back-up power.
Inadequate/Missing Power Alarm
System failure associated with an un-alarmed (or under-alarmed) power failure, an alarm not provided initially due to inadequate standards, failure to implement standards or an alarm/alarm system failure (broken or modified). Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as Procedural failures.
Insufficient Response to Power Alarm
System failure associated response to power failure: alarm system worked, but support personnel did not respond properly.
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 resulting from infrequent power system testing, maintenance and/or detailed inspection.
Other
Overloaded/Undersized Power Equipment
System failure attributable to insufficient sizing/design of power configuration.
Rectifier Failure
System failure resulting from rectifier malfunction.
Scheduled Activity-Software Upgrade
Scheduled Maintenance-Hardware Replacement
Unidentified Power Surge
Equipment failure associated with unidentified power surge.

Procedural - Other Vendor/Contractor

Ad hoc Activities, Outside Scope of MOP
Unapproved, unauthorized work, or changes in agreed-to procedures.
Documentation/Procedures Out-of-Date, Unusable, Impractical
Lack of updated documentation/procedures, the correction/update is available but not incorporated locally, or the document is unwieldy. Some examples are: the use of inadequate indexing or cross-referencing, bits and pieces of information being too difficult to integrate, ineffective delivery vehicle, etc.

Documentation/Procedures Unavailable, Incomplete

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

Insufficient Staffing/Support

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

Insufficient Supervision/Control or Employee Error

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

Insufficient Training

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

Other

Procedural - Service Provider

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

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

Documentation/Procedures Unavailable/Unclear/Incomplete

Documentation or procedures (vendor or service provider) are not published; published, but not distributed; distributed, but not available on-site, etc.
Documentation/procedures are obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

Inadequate Routine Maintenance/Memory Back-Up

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

Insufficient Staffing/ Support

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

Insufficient Supervision/Control or Employee Error

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

Insufficient Training

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

Other

Procedural - System Vendor

Ad hoc Activities, Outside Scope of MOP

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

Documentation/Procedures Out-of-Date Unusable or Impractical

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

Documentation/Procedures Unavailable/Unclear/Incomplete

Documentation or procedures (vendor or service provider) are not published; published, but not distributed; distributed, but not available on-site, etc.
Documentation/procedures are obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

Insufficient Staffing/ Support

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

Insufficient Supervision/Control or Employee Error

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

Insufficient Training

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

Other

Simplex Condition

Non-service Affecting

Occurs when there is a failure of one side of a duplexed system such as a SONET ring yet an unprotected simplex service will still provide service for the duration of the outage.

Do not use this root cause for the complete failure of a duplexed system or in cases where any of the circuits in the duplexed system are provided under Service Level Agreements (SLAs) which require protection.

Service Affecting

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

Spare

Spare Not Available – Sparing processes did not result in an available replacement (e.g., service provider inventory inaccuracies, transportation of spare located at centralized facility, etc.). However, if the unavailability is due to equipment beings Manufacture Discontinued, the cause should be listed
as **Spare On Hand - Manufacturer Discontinued (MD)**

Spare On Hand – Manufacturer Discontinued (MD)

Obtaining spare made difficult or complicated by MD status (e.g., service provider unaware of MD status, scarcity of MD spares, etc.).

Spare On Hand – Failed

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

Traffic/System Overload

Common Channel Signaling Network Overload

SS7 system/network overload associated with (true) high traffic loads congesting signaling network elements or the SS7 link network. If the overload was associated with signaling traffic handling congestion, false or reactivated link congestion, inappropriate or incorrect SS7 network management message(s), protocol errors, etc., then consider the problem to be a Design - Software fault.

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

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

Ineffective Engineering/Engineering Tools

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

Mass Calling - Focused/Diffuse Network Overload

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

Media-Stimulated Calling - Insufficient Notification

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

Other