1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

May 26, 2017

Via Email
Jeffery Goldthorp
Associate Bureau Chief for Cybersecurity and Communications Reliability
Public Safety & Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Room 7-A325
Washington, D.C. 20554

Dear Mr. Goldthorp:

The ATIS Network Reliability Steering Committee (NRSC) met and reviewed the implementation of the new NORS 3.0 platform. NRSC member companies have identified the following areas that warrant additional attention. This feedback falls into two categories: (1) those issues requiring immediate Commission attention for NORS 3.0; and (2) more general feedback for future changes to NORS.

Issues Requiring Immediate Attention:

- Challenges associated with user management and user setup problems, including the inability to: (1) manage permissions; (2) add users; and (3) change user profile (i.e. name, phone numbers). This functionality is necessary and should be implemented

- Known bugs associated with filing outage reports in NORS 3.0 must be corrected, including:
    - Not all filed reports are visible in NORS 3.0 (filed Notifications with receipt emails are not visible in NORS 3.0 when users try to file an Initial Report);
    - Some users are unnecessarily required to log in more than once for a session;
    - The "reason reportable" field does not include all appropriate options ("DS3" and "Transport" type outages are not provided in NORS 3.0 as options);
    - When a notification report is filed, the person who filed the report (inputter) does not receive a confirmation (only coordinators receive the confirmation email);
    - When a request to re-open a report is made, there is no confirmation of the request (under previous version of NORS, an instant notification was sent via e-mail);
    - Despite not being required by the Commission's outage reporting rules, Initial Reports for VoIP outages are required in NORS 3.0 in order to file a Final Report;
    - The "auto-population" function does not work for secondary contacts;
    - The secondary contact field is not searchable/cannot be added (i.e., the "search" field does not work);

  - The "from" field in NORS-related emails (i.e.: IT Service Desk <fccprod@midatl.service-now.com>) is confusing as it does not indicate that the email is being sent by the Commission. The NRSC recommends that the "from" field indicate the e-mail is from the Commission (i.e. IT Service Desk@fcc.gov); and
  - Previously one could extract a copy of the most recently filed report, save this copy on his/her computer and make updates to the sections that had updates. This was generally used when filing the Initial or Final reports and was part of a company's internal review and approval process of all NORS filed reports. The inability to use an existing report and make updates requires one to create a template and retype all information over again for these internal reviews.

- The reporting capabilities of NORS 3.0 are incomplete and must be enhanced:
  - A list of all open reports is no longer available (this is the most common report used daily by NRSC member companies); this function used to be available via a button on the main screen;
  - Upcoming reports (reports due in 5 days) are no longer available; this function was valuable in ensuring compliance with deadlines;
  - Report due dates are no longer visible;
  - Overdue reports cannot be exported;
  - The ability to filter results based on specific date ranges is not available (under previous NORS versions, users could apply filters to all fields, including date); and
  - The ability to view only the most recent version of a report is desired; however, previous iterations of a report should be kept for historical reference purposes.

Long Term Feedback

- In the past, the industry has been given time to accommodate new processes/automation in new version of NORS. However, the transition to NORS 3.0 provide only a minimal amount of transition time and there was inadequate notification/time available for training (from the Commission, and internal within NRSC member companies).
- ATIS NRSC also notes that the production code for NORS 3.0 was not the same as test code, resulting in confusion. ATIS NRSC recommends that the Commission ensure that the test environment is as close to the production environment as possible for future revisions to NORS.
- The NRSC recommends that the Commission add an additional level for user access for custodians or additional company managers/contacts who may approve user access for a given company. This new level (with administrative permission) would allow companies to solve issues without contacting the Commission.
- The NORS 3.0 platform is comparatively more cumbersome than previous versions. The NRSC recommends that the Commission work to make future versions more user-friendly.

- ATIS NRSC remains concerned that changes and problems associated with NORS 3.0 have not communicated effectively by the Commission. More timely and frequent communications about these changes/problems would allow the industry to be better prepared for future implementations.
- The Commission does not appear to have established a standard maintenance window for NORS 3.0 and/or information on maintenance was not communicated to the industry. activity is not communicated
- The Commission did not uniformly address carrier issues with the system or communicate their responses (some filers had their questions answered immediately, while others never received a response).
- In the SOAP interface, date and time format must be changed before updating a report ("T" is inserted)

ATIS NRSC urges the Commission to expeditiously address these issues, particularly those challenges/bugs that are frustrating members' attempts to input and update notifications/reports in a timely and efficient manner. ATIS NRSC further notes that some member companies are choosing to manually upload outage reports to overcome the bugs that currently exist in the NORS 3.0's automation tools.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Tom Goode
ATIS General Counsel

1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

May 26, 2017

Via Email
Jeffery Goldthorp
Associate Bureau Chief for Cybersecurity and Communications Reliability
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, SW
Room 7-A325
Washington, DC 20554

RE: NRSC Feedback on DIRS and the DIRS Activation for Hurricane Matthew

Dear Mr. Goldthorp:

On behalf of its Network Reliability Steering Committee's (NRSC) Outage Reporting Advisory Subcommittee (ORAS), the Alliance for Telecommunications Industry Solutions (ATIS) is writing to provide you with NRSC ORAS' feedback on the Disaster Information Reporting System (DIRS), the DIRS User Manual, and the 2016 DIRS Activation for Hurricane Matthew.

DIRS/ DIRS User Manual Recommendations:

- NRSC recommends that the Commission modify the DIRS upload file size limitation (i.e. 60K), and/or allow service providers to upload compressed (e.g. .zip) files (NRSC recommends that the FCC also consider file sharing technology).

- NRSC recommends that the Commission send all submission errors related to an upload attempt in a single email (rather than in separate emails one error at a time).

- NRSC recommends that the Commission inform stakeholders of an anticipated activation of DIRS for a general area in advance of an activation of DIRS and to designate specific counties in a disaster area. This would be useful for service providers to prepare for reporting in a general area.

- NRSC recommends that the Commission ensure all DIRS coordinators are aware of the capability to receive SMS text messages in addition to e-mails for all DIRS activations/deactivations. NRSC notes that this capability would enhance notification effectiveness after hours or on weekends.

DIRS Activation for Hurricane Matthew Feedback:

- NRSC observed that after Hurricane Matthew, wireless carriers were contacted by the Commission to provide data that is not part of a normal DIRS activation, namely data concerning wireless calls by each evacuation area before, during, and after the disaster. Requests for additional data outside of normal DIRS reporting present challenges, particularly when the request seeks information for which real-time data may be unavailable and/or requires providers to pull information from

archived data (e.g. equipment logs). The challenges are exacerbated when relatively short deadlines are provided.

- NRSC would like to understand the rationale for the Commission's decision to deactivate Hurricane Matthew DIRS reporting for most companies and not for others (i.e. cable companies). NRSC recommends that DIRS be uniformly activated/deactivated for all affected service providers and industry segments without exception.

- While NRSC ORAS does not believe that information released during Hurricane Matthew violated the Commission's duty to maintain confidentiality of sensitive outage data, NRSC is concerned with the publication (i.e. FCC webpage information release) of certain aggregated DIRS data. In some instances, releasing data on specific counties by service type is tantamount to releasing the service provider's identity.

If you have any questions or need additional information, please do not hesitate to reach out.

Sincerely,

Tom Goode, ATIS General Counsel (tgoode@atis.org)

CC: John Healy (john.healy@fcc.gov)
Julia Tu (julia.tu@fcc.gov)
David Ahn (david.ahn@fcc.gov)
Andy Gormley, NRSC Co-Chair (andy.gormley@t-mobile.com)
Andis Kalnins, NRSC Co-Chair (andis.i.kalnins@verizon.com)
Jackie Wohlgemuth, ATIS Global Standards Development Manager (jvoss@atis.org)

NRSC Bulletin No. 2017-002

"Silent Alarm Failures" Investigation

March 2017

Background

The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) has been investigating a concern raised by the FCC associated with what is perceived to be outages that are not detected by equipment alarming (e.g., non-intrinsic alarming for translation failures, input errors, etc.). The NRSC has reviewed the issue and determined that some existing industry recommendations can be provided to reduce the frequency of these failures from occurring and mitigating the impact of these types of failures if they do occur.

Methodology

NRSC members examined the examples of "Silent Alarm Failures" provided by the FCC and also looked at additional examples internal to their respective companies. The Committee held a series of meetings to discuss and compile the individual findings and to provide a consensus of the issues and concerns around these events. The examples were investigated and the applicable Best Practices were provided to form a comprehensive list of practices aimed at reducing the frequency of these types of outages and mitigating their impacts when they do occur. Given differences in NRSC member networks and technologies (i.e., vendors, frameworks, services provided, surveillance equipment, infrastructure, etc.), this general approach seems to be most applicable to operators and carriers.

Findings

The NRSC initiated a general review of Best Practices related to alarming and each member company initiated an internal review of their respective alarming practices. The NRSC found that the events around "Silent Alarm Failures" generally are attributed to situations that dealt with new technology, where existing processes and procedures did not anticipate the particular situation that occurred. Once these situations were identified, Root Cause Analysis (RCA) reviews were routinely conducted and the existing alarming, triggers, Key Performance Indicators (KPIs), and/or Methods of Procedures (MOPs) were modified to address identified issues. The NRSC recognizes that a vast number of alarm states from equipment software exist for carriers to utilize and must be filtered to enable an appropriate response from the service provider operating centers. These alarms range from minor in nature, but still alert carriers to non-critical events on the network, to service-affecting events to which carriers must focus their attention. Service providers must employ software options to trigger meaningful alarms through the interconnected nodes of their operating systems. There is no evidence pointing to a common primary contributor within the data collected from the NRSC or the FCC.

Recommendations

The NRSC recommends that Network Operators, Service Providers, Public Safety, and Equipment Suppliers review the findings of this Bulletin and revisit the Best Practices in this Bulletin and continue to implement those that are applicable, which will contribute to the reduction of "Silent Alarm Failures". The

following Best Practices were selected from the existing Best Practices and were found to be applicable to the events that were reviewed, plus additional Best Practices suggested by NRSC members. These Best Practices address areas related to “Silent Alarm Failures”.

The NRSC recommends that in addition to reviewing Best Practices, carriers consider conducting a periodic review of their existing alarming, triggers, KPIs, and/or MOPs, as appropriate and recommends a new Best Practice: Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct regular review of their alarming thresholds and selection.

The general NRSC recommendation for service providers is to provide a more proactive investigation of new MOPs and to provide regular reviews of existing alarming, particularly around evolving technologies.

Number	Best Practice
9-5-0514	When available, Network Operators and Service Providers should utilize a management system capability (e.g., Common Object Request Broker Architecture [CORBA], Simple Network Management Protocol [SNMP]) providing a single interface with access to alarms and monitoring information from all critical network elements.
9-9-0602	Network Operators and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).
9-9-0612	Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.
9-6-0761	Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds, and alarms.
9-6-5235	Network Operators, Service Providers, and Equipment Suppliers should ensure that impacted alarms and monitors associated with critical utility vaults are operational after a disaster event.

NRSC recommends the following new Best Practice:

Recommended Addition	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct regular review of their alarming thresholds and selection.