Before The
Federal Communications Commission
Washington, D.C. 20554

In the Matter of

Improving 9-1-1 Reliability PS Docket No. 13-75

COMMENTS OF ASSURE911.NET, LLC

ASSURE911.NET, LLC respectfully submits these comments, pursuant to the Federal Communications Commission’s ("Commission") Notice of Proposed Rulemaking (FCC 13-75) ("Notice")\(^1\).

The Commission, in the Notice in paragraph 7\(^2\), has clearly stated the goal for 911 reliability is end-to-end, from originator to the call taker. We heartily agree.

In the Notice in paragraph 66\(^3\) the Commission introduces the term 911 Network Operations Center (NOC) providers, and describes their role, including what to do during adverse events. We agree that this role for a given PSAP should fall to the responsible Covered 911 SSP who is recognized by local or state authorities as being responsible for delivery of calls to that PSAP, whether that be an ILEC, an ESI.net provider, or a covered 911 SSP so designated by the jurisdiction. We envision the

\(^2\) NOTICE, II A, 7, Page 4
\(^3\) NOTICE, IV D. 66, Page 27
configuration in which the designated 911 NOC provider, as an ESInet provider, has assumed responsibility for the complete transport of 911 call traffic into their NG9-1-1 Network Architecture, and then on to their PSAP client call taker systems, as well as all database services for their PSAP client base. That ESInet provider may have contracted out the underlying broadband network services, as well as trunks and facilities from the originating networks, and data links from the database services providers. Such a covered 911 SSP would consider it good business practice to have in hand all of the data about the health and status of the components being used to bring 911 calls to their systems. For 911 services that are supported on their behalf by their contracted suppliers, it makes sense to have that data on a continuous proactive basis. The proposed rule changes will help by clearly requiring that any service impacting the end-to-end call processing environment, from caller to PSAP, will have a reporting agreement to the designated 911 NOC Service provider. The service exceptions should be reported as close to real time as possible, preferably electronically and followed up by the NOC Provider. This could take the form of setting up communications such as a conference bridge or similar mechanism to work on the problem, and ascertain the reportability of the incident, notify the correct local, state, and federal parties, as well as the PSAP affected by an event. We can envision another configuration, similar to the State of Washington outage event, in which a single provider of transport, functional elements or database services could affect several designated 911 NOC Providers across many PSAPs and therefore an outage in their environment would require an even higher level of alerting, notification and restoration coordination. Even in this case we
see value in having entities designated as 911 NOC providers, coordinating and working with others for even a single jurisdiction. If a serious outage requires a large single business entity to communicate with many of their customers, or even “all” of their customers, that seems an appropriate function of such an entity. There will be ESInet to ESInet connections that cross many boundaries in the future. These boundaries may be PSAP to PSAP, inside States between 911 SSPs, County-to-County, or State-to-State. Where interstate agreements are needed, the Commission has a unique role in establishing rules and responsibilities between equal parties in the event of an outage. Some protocols ought to be established in advance for coordination and notification. In our observations ESInet to ESInet connectivity between states will be coming soon if it has not happened already. Simple rules could resolve finger pointing or a situation where no one or everyone is required to take action.

We therefore agree with the need for this designation and the concept of sharing information by other Covered 911 Service Providers so that 911 NOC provider can have situational awareness during outages. The need for this became clear to the members of Assure911.net, LLC long before our founding, when at previous positions we developed and implemented 911 reliability systems for the CLEC environment. Our company was more recently founded in order to get out this very message to the emerging Next Generation 911 industry that sharing of information about adverse events is a critically important aspect of end-to-end reliability and we support the adoption of the rules surrounding the 911 NOC provider. We do have recommendations to make about alarming and which entities should be required to
share information.

In the Notice in paragraph 42\(^4\) the Commission proposes to exclude providers of originating 911 calls as a Covered provider, and at first reading we feared that the goal of end-to-end reliability would be as a result unachievable. The 911 calls originate from carrier networks as clearly noted in the diagrams in the opening comments of the Notice. Reliability also originates from the caller, the one party whose perception of reliability is the most important. Providers of originating services become aware of failures of the individual calls attempts that do not reach any PSAP call taker. It is our experience and belief that exception and failure data emanating from the originating services provider network elements, when collected in real-time and acted upon promptly, is just as an effective a resource for achieving reliability as physical diversity end-to-end across the 911 network architecture and networks. Upon reflection we can agree that is not necessary to define such providers under the newly proposed changes to definition in 12.4 (a) (4) (i), however we strongly recommend that a role in 911 reliability be clearly defined for providers of 911 emergency origination services.

We recommend that providers of 911 originating calls and text messages have the responsibility to provide to the appropriate 911 NOC Provider information from their networks which represent failures to communicate to 911 across any point in the network they own or manage. They may not be the 911 SSP, but they may be responsible for transport elements along the call path to an ESI(s) diversely or to

\(^4\) NOTICE IV A. 42, Pages 18,19
the PSAPs diversely. If in fact the originating service providers do not participate, the first points of failure could well be non-diverse trunking to the ESInet from an end office or Host. We do recognize that Remote Central Offices seldom have an alternate access path and 911 is impaired if their host, or umbilical to the host, is impaired. That is the same for a LEC, ILEC, CLEC or MSC. The more rural the caller, the lower the probability they would be diversely connected to a PSAP. This is true today especially where Selective Routers are in use and will be true in NG9-1-1 deployments that leave the legacy Selective Routers in place.

In the Notice in paragraph 45\(^5\) and the footnote thereto the Commission correctly points out that alarms related to calls that are not being processed or completed are critical and should be included in network monitoring, just as an entity would monitor physical facilities. In providing examples of how an entity might compare peg counts to derive to the portion of attempts that are failing the Commission is correctly advising on best practices for those entities who are responsible for only a part of the end-to-end path. We would point out that the alarms directly indicating actual individual attempt failures, not derived events, are readily available from the networks of the providers of originating services today, and recommend that the Commission require that these providers share this information with the responsible 911 NOC Provider.

The failures may be due to issues in the originators network. In this case the information would only be used by the responsible 911 NOC Provider to fulfill their

\(^{5}\) NOTICE IV A. 45, Page 20
responsibility to notify the PSAP. In cases where the failures are due to issues in the network or systems of the 911 NOC Provider, or in the networks and systems of any of the Covered 911 SSPs who are included by contract, the shared information would be used to both notify and initiate troubleshooting.

Further, when discussing thresholds, we point out that from the perspective of the call originator, the “substantial portion” of their call attempts is as little as one (1), and recommend that an alarm be generated when the first failure occurs. Thresholding and suppression should only be applied to subsequent, “similarly impacted” failures that occur after the first failure. “Similarly impacted” call attempts are those attempts that are failing from the same group of subscribers for the same reason. A group of subscribers is meant to be those whose calls would be routed from various call origination points to the same PSAP. Call attempts originating from each separate group of subscribers in each point where calls originate, such as each local end office, a collection of cell sites whose calls are aggregated and trunked to the same mobile switching office, and VoIP POIs, can be considered from the same area and alarmed once, upon the first occurrence. Typical NOCs would not be interested in a single failure. However when it comes to 911, every failure is an important indicator of trouble that must be acted upon. A 911 NOC is unique. If a provider treats their failed 911 calls like non-emergency call failures, then a significant number of failures will have to occur and break a threshold to be noticed.
In the Notice in paragraphs 70 through 72\textsuperscript{6} the Commission seeks comment on the manner in which data is to be shared, the nature and content of the shared data. It is our view that sharing timely and adequate information should be done on a continuous and pro-active basis not solely during an outage. This is best achieved by automating the delivery of useful information. We believe it should be the responsibility of the designated 911 NOC providers to aggregate the data, such as reports from their own systems, or the collected reports from systems of any originating access, signaling, database, or transport providers from whom they or their jurisdictional clients contract for services. This data in turn can be used to create useful situational awareness for all, including the impacted PSAPs. We do acknowledge that the industry may have a reluctance to share sensitive outage information with potential competitors, however in this environment the recipient of the data in question is actually a customer. A customer as it happens, who has a regulated responsibility to keep all aspects of 9-1-1 service operating. Given the recent events described in the Notice, the critical nature of sharing the knowledge that citizens may not be able to reach 9-1-1 we would not expect any reluctance.

The Commission could establish a rule that supports the \textit{automatic} notification from all Covered SSPs to the designated 911 NOC provider about an adverse condition in which useful, actionable information would be provided. An example of a minimum set of relevant data and the events that should trigger transmission of the data are shown in the table below. Essentially, the trigger for sending data is any occurrence

\textsuperscript{6} NOTICE, IV D. 70, 71, 72, Pages 28,29
that will interfere with the next communication attempt on the end-to-end path to the PSAP from any of the points where it may originate.

<table>
<thead>
<tr>
<th>Trouble Type</th>
<th>Relevant Data: Estimated Time of Restoral, and</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolations</td>
<td>End office, carrier, NPA-NXX-line range or cell site(s) effected</td>
</tr>
<tr>
<td>Call failures</td>
<td>Calling Party Number or From URI, or Geo-Location of originator</td>
</tr>
<tr>
<td>Selective Router Failure</td>
<td>End offices, carriers, NPA-NXX-line range or cell site(s) effected</td>
</tr>
<tr>
<td>NG911 Core Functional Element Failure</td>
<td>End offices, carriers, NPA-NXX-line range or cell site(s) effected</td>
</tr>
<tr>
<td>Degraded Service due to Facility Failure</td>
<td>End offices, carriers, NPA-NXX-line range or cell site(s) effected</td>
</tr>
<tr>
<td>Degraded Service due to Overload</td>
<td>End offices, carriers, NPA-NXX-line range or cell site(s) effected</td>
</tr>
</tbody>
</table>

Table 1 – Relevant Data to be collected by the designated 911 NOC

In the table above the events and estimated time of restoral can only be detected and provided by the parties responsible for the facilities in which the trouble occurs. Enumerating the relevant data, such as the impacted subscribers, can be accomplished either by the parties in whose facilities the trouble occurs, or preferably, by the designated 911 NOC provider, by use of their own configuration management platform.

The question may arise as to the cost impact of imposing additional reporting requirements. The emerging NG9-1-1 systems may require additional, non-standard features to implement the proposed rule changes, but these can be minimally folded in to the cost of deployment of the NG9-1-1 system or ESI/net. In the case of existing Selective Router based 9-1-1 systems, the cost to a provider for sharing this data is also expected to be minimal. Most entities already collect data representing the above triggers when they occur, with systems that allow electronic forwarding of such collected data. For entities that may not be using their systems in this manner, or lack the expertise to implement this capability, products and services to aid them are abundant in the industry.
We respectfully suggest amending the proposed changes as indicated below.

**Replace 12.4 (a)(4)(ii) B, with:**

Communications providers that solely originate voice calls or text messages to 911 but do not provide any of the capabilities or services described in subparagraph (i) of this subsection. These providers are however considered as Origination Service Providers as defined in 12.4 (a)(12).

**Add Paragraph 12.4 (a)(12) to read as follows:**

(5) *Origination Service Providers.*

i. Any entity that:

(A) Provides the origination of voice calls, text messages, or any communications attempts to 911. These providers may function in other roles defined in section 12.4.

**Add Paragraph 12.4 (c)(3)(iii) to read as follows:**

An Origination Service Provider shall provide to the Designated 911 NOC Providers, information about their networks reflective of failures to communicate to the 911.

   (A) The Origination service provider shall provide information to the designated 911 NOC provider on adverse conditions, such as isolations, call attempt failures, and Trunk, Circuit, or Facility Failures in the end to end path from a calling area to the PSAP.

   (B) The Origination service provider shall provide information to the designated 911 NOC provider on a continuous, proactive basis.

   (C) The Origination service provider shall provide information to the designated 911 NOC provider on automated basis.
Statement in support of the need for rules regarding sharing data

The typical NOC is disappearing as companies go to more distributed problem solving by specialists on an equipment type not a service type or category. We find that with providers with whom we work today. Ethernet services are managed by an entirely different workforce than SONET failures, potentially in a different state. TDM Switches are managed by a different NOC, often by vendor make and model, such as a Genband Nortel group of NOC technicians or an Alcatel Lucent group of NOC technicians, or SS7 components, ISDN and CAMA trunks. 911 Databases are another 911 special issue. The data links for queries may be actively monitored and troubles with them reported by the database query service provider, but it could be an ILEC who is the first to notice failures. The PSAP quite often the very first to know the addresses or location information is not available. With the E911 database link for VoIP and wireless, carriers are connected individually, with a direct link to each PSAP. With NG9-1-1, the database links to providers of ALI query services connect to diverse Data Center Equipment in at most two (2) locations however large of a geographic area the ESInet may support. The MSAG Database is housed in diverse data centers if the NG9-1-1 network was built with diversity. These seemingly small technical issues are big issues if not alerted and managed properly.
Additional discussion about the Role of the Designated 911 NOC provider

The designated 911 NOC provider should have the ability to alarm and gather data related to 911 exceptions and alert the designated parties that can resolve the problem.

An operational method should exist for escalation to the responsible parties in the end-to-end process. Analyses and resolution of the problem must begin on receipt of actionable information. The responsible parties include those who can trigger automatic or manual transition to the diverse and reliable back up arrangement if it did not occur already.

If the problem is simplex, use tools to isolate and bring the proper parties together to restore service. Many states such as Illinois require notification if a simplex condition exists. Know who is responsible to ascertain the simplex condition and notify the appropriate parties and start to open tickets and use the escalation notification process.

Ensure the PSAP(s) are aware of the situation. As close to the start of resolution and isolation of trouble as possible, ensure the PSAP, if impacted, has the opportunity to use their alternative back up arrangements, call out extra personnel and/or activate an emergency backup plan if needed while the network is being restored to full duplex operation. With non-emergency communication, simplex outages require no such elaborate measures. In NG9-1-1, if the ESI.net and Database access network are built and tested to complete standards, it should be seldom that any manual
intervention will be required in a simplex outage, however we believe it is good practice to make relevant parties aware.

If the condition is duplex, alert all necessary parties. The State and the Commission have criteria to determine at what points regulatory reporting is required. The designated 911 NOC provider must track daily call volumes and be aware of the number of supported citizens in the geography, and should be able to readily reference that information to make reports in a timely manner, in addition to notifying affected PSAPS. In the case of NG9-1-1, backup PSAPs ought to be able to receive and process the calls readily without manual intervention. Access to the same database records as the original PSAP is needed, thus preserving availability of location information. If the backup PSAP has to use an alternate means to dispatch, access to that information needs to be pretested and prove ready to be used immediately when the first calls arrive. Staffing of the PSAP may be an issue. The management of the backup PSAP that starts receiving calls ought to be notified of adverse events as well, and right away, to be in a position to augment staff if required.

As always if the Border Control Function is in place as it ought to be in any standard NG9-1-1 network, thresholds can be adjusted if needed to allow calls to flow and be handled in a different manner.

The Notice assumes load balance. This issue is another manner and in some cases vendors do not support load balance as described. More work must be done since SIP does not automatically load balance calls. Network engineering rules and
requirements are necessary and they must be agreed upon with all carriers from start through to finish of the end-to-end network design.

The Notice addresses certification that does not exist at this point either. NENA ICE is an excellent start toward certification but is not there yet and many vendors do not participate in ICE, or participate minimally. No one is required to say who passes and who fails and in fact the rules require confidentiality of all details.

Any system built to support sharing of automated situational awareness information need not have additional troubleshooting features, such as a traffic reporting or protocol analysis platform. These and many other useful tools that can to be deployed for NG9-1-1 SIP testing are available off-the-shelf.

The monitoring and automated sharing of alerts could however, be set up as a means of automatically reporting to the state or interfacing directly to the Commission’s systems. A qualified person should look at the outage alert information and make a qualified decision as to the appropriate timing and need for a report to either the Commission the state or simply add to the PSAP notification. All of this is technically possible. The proposed changes will instill a sense of urgency to do this now. We have laid out the initial requirements for this type of interface and report capability.
Conclusion

The Commission should require providers of Origination Services to contribute to situational awareness.

a) The Origination service provider shall provide information to the designated 911 NOC provider on adverse conditions, such as isolations, call attempt failures, and Trunk, Circuit, or Facility failures in the end-to-end path from a calling area to the PSAP.

b) The Origination service provider shall provide information to the designated 911 NOC provider on a continuous, proactive basis.

c) The Origination service provider shall provide information to the designated 911 NOC provider on automated basis.

Respectfully submitted,

/s/

________________________
Barbara Kemp
Partner
Assure911.net, LLC
bk@assure911.net
(847) 778-2874 phone

/s/

________________________
David Staub
Managing Partner
Assure911.net, LLC
dbs@assure911.net
(860) 620-7735 phone

March 10, 2015