911 Reliability Webinars

Federal Communications Commission

Public Safety & Homeland Security Bureau

July 16, 2014

August 13, 2014

September 10, 2014

Important Point

- This presentation summarizes the ***911 Reliability Report and Order*** adopted by the Commission in December 2013.
  - The *Report and Order* is published at **28 FCC Record 17476** and available online at http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db1212/FCC-13-158A1.pdf.
  - Relevant rules are codified at **47 C.F.R. § 12.4**.
- The *Report and Order* reflects the Commission's official decision and supersedes the overview provided here. If in doubt, please consult the **actual text of the rules**.
  - Please direct any questions about interpretation of the rules to PSHSB staff and/or your legal counsel.

911 Reliability *Report and Order*

- Adopted December 2013 in response to preventable 911 outages during **June 2012 derecho storm**
- **Covered 911 Service Providers** must take **reasonable measures** to provide reliable service, as evidenced by an **annual certification** of compliance with best practices or reasonable alternative measures.
  - **Critical 911 circuit diversity**
  - **Central office backup power**
  - **Diverse network monitoring**
- If a service provider relies on alternative measures or claims that a portion of the certification is not applicable to its network, it **must provide a brief explanation**.
- PSHSB has **delegated authority** to administer certification process, develop and revise forms, review certification information, and order remedial action if necessary.

Covered 911 Service Providers

- Any entity that:
  - **Provides 911, E911, or NG911 capabilities** such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent, **directly to a public safety answering point (PSAP)**
    - Does **not** include PSAPs or governmental authorities
    - Does **not** include communications providers that originate 911 calls where another provider delivers those calls and ALI/ANI to the appropriate PSAP
  - **Operates a central office that directly serves a PSAP**
    - A central office **directly serves a PSAP** if it hosts a selective router or ALI/ANI database, provides equivalent NG911 capabilities, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP.

Certification Elements: Critical 911 Circuit Diversity

- A Covered 911 Service Provider shall certify whether it has, within the past year:
  - **Conducted diversity audits of critical 911 circuits** or equivalent data paths to any PSAP served
    - **Critical 911 circuits** defined as facilities that originate at a selective router or its functional equivalent and terminate in the central office that serves a PSAP, including links to ALI/ANI databases
  - **Tagged critical 911 circuits** to reduce the risk of inadvertent loss of diversity between audits
  - **Eliminated all single points of failure** in critical 911 circuits or equivalent data paths serving each PSAP.
    - If not possible to eliminate single points of failure, the provider must include a brief explanation of **alternative measures or ongoing remediation**, the date by which it anticipates remediation will be completed, and why it believes those measures are reasonable under the circumstances
    - May respond that this section is **not applicable** if an entity does not operate any critical 911 circuits (e.g. provides only a PSAP's 10-digit administrative lines but not its selective router(s) or location database(s))

Certification Elements: Central Office Backup Power

- With respect to any central office that directly serves a PSAP, a Covered 911 Service Provider shall certify whether it:
  - **Provisions backup power** through fixed generators, portable generators, batteries, and/or fuel cells to maintain full-service functionality, including network monitoring capabilities:
    - For at least **24 hours** if the central office directly serves a PSAP
    - For least **72 hours** if the central office hosts a selective router
  - **Tests and maintains** backup power equipment in accordance with the manufacturer's specifications
  - Designs backup generators for **fully automatic operation** and for **ease of manual operation**, when required
  - Designs, installs, and maintains each generator in any central office that is served by more than one backup generator as a **stand-alone unit** that does not depend on the operation of another generator for proper functioning
  - May certify **alternative measures** or **non-applicability**, but must provide a brief explanation.

Certification Elements: Diverse Network Monitoring

- A Covered 911 Service Provider shall certify whether it has, within the past year:
  - **Conducted diversity audits** of its **aggregation points** for network monitoring data in each 911 service area and of the **monitoring links** between such aggregation points and its network operations center(s) (NOCS)
    - **911 service area** is defined as the geographic region in which a Covered 911 Service Provider operates a selective router or the functional equivalent
  - **Implemented physically diverse aggregation points** for network monitoring data in each 911 service area and **physically diverse monitoring links** from such aggregation points to at least one NOC
    - If not possible to implement physically diverse aggregation points or monitoring links, the provider must include a brief explanation of **alternative measures or ongoing remediation**, the date by which it anticipates remediation will be completed, and why it believes those measures are reasonable under the circumstances
    - May respond that this section is **not applicable** if a provider does not operate a selective router or the functional equivalent (i.e. no "911 service area" to monitor)

Status and Effective Dates

- Rules that do not require Office of Management and Budget (OMB) approval (e.g. "reasonable measures" requirement) took effect **February 2014**.
- **Initial and annual certifications** involve a collection of information that must be approved by OMB.
  - OMB approval expected approximately **September 2014**.
  - Initial certification of at least 50-percent compliance with each element expected approximately **September 2015.**
  - Full annual certifications due **every year thereafter** (e.g. approximately **September 2016**).
- **Petition for Reconsideration** filed February 2014 involving certification obligations of Next Generation 911 (NG911) providers and responsibility for auditing facilities leased from third parties
  - Petition is still pending
  - Comments were due by March 27 and replies by April 7
  - Further views should be filed in **PS Docket Nos. 13-75 and 11-60**

Break for Questions

- *Report and Order* and rules:
  - Eric Schmidt
    Attorney Advisor
    Cybersecurity and Communications Reliability Division
    (202) 418-1214
    eric.schmidt@fcc.gov

Certification Process

- Data will be entered through an **electronic portal** similar to the FCC's Network Outage Reporting System (NORS).
- Small providers with only a few PSAPs/central offices can enter data for each location in an **online form**.
  - Proposed forms are under OMB review and may be subject to change.
- Larger providers with many PSAPs/central offices can enter summary information in the online form and upload details for each location in an **Excel spreadsheet**.
- System will provide **drop-down menus** of common alternative measures with a free-text option for "other."
- Certification must be attested under penalty of perjury by a **corporate officer with supervisory and budgetary authority** over network operations in all relevant service areas.
  - System will allow service providers to upload an attestation letter after entering certification data.

Certification Information

- Materials submitted with a certification will be **presumed confidential** to the extent that they consist of:
  - Descriptions and documentation of alternative measures
  - Information detailing specific corrective actions
  - Supplemental information requested by the Commission or Bureau
- Fact of filing (or not filing) a certification and aggregated information about a provider's responses **will not be treated as confidential**.
  - PSHSB may periodically release public reports summarizing information received in a certification period without disclosing confidential information.
- Service providers are **encouraged to share relevant circuit audit records with PSAPs** on reasonable terms that protect confidentiality of proprietary information.

Certification Form Examples

(Under OMB Review; May Be Subject to Change)

Critical 911 Circuit Diversity

Within the past year, has the certifying entity:

a) Conducted diversity audits of critical 911 circuits or equivalent data paths to every PSAP served,
b) Tagged such critical 911 circuits to reduce the probability of inadvertent loss of diversity in the period between audits, and
c) Eliminated all single points of failure in critical 911 circuits or equivalent data paths serving each PSAP?

- ☐ Yes for all PSAPs. Please fill in the report which lists all PSAPs with certified diverse circuits.
- ☐ Yes for some PSAPs but alternative measures for other PSAPs. Please fill in the report which lists all PSAPs with certified diverse circuits. For each PSAP with alternative measures implemented, please provide those alternative measures using the "Alternative Measures for Diversity Audit of Critical 911 Circuits" report.
- ☐ No, but alternative measures for all audited PSAPs. For each PSAP with alternative measures implemented, please provide those alternative measures using the "Alternative Measures for Diversity Audit of Critical 911 Circuits" report.
- ☐ No. Please explain:
- ☐ Not applicable. Please explain:

Alternative Measures for Diversity Audit of Critical 911 Circuits

PSAP name:

State (chose from menu): -AK -AL -AR -CA

County Name:

Diversity Audit Conducted: - Yes - No

Reason Diversity Audit Not Conducted:

911 Circuits Tagged: - Yes - No

Reason 911 Circuits not Tagged:

Reasons Not Fully Diversified (chose from menu):
- Alternative Measure 1
- Alternative Measure 2
- Alternative Measure 3
- Other

If "Other" Reason Selected Above, Describe Why Critical 911 Circuits Are Not Fully Diversified:

Certification Form Examples

(Under OMB Review; May Be Subject to Change)

Central Office Backup Power

With respect to any central office that directly serves a PSAP, does the certifying entity:

a) Provision backup power through fixed generators, portable generators, batteries, fuel cells, or a combination of such sources to maintain full-service functionality, including network monitoring capabilities, for at least 24 hours at full office load or, if the central office hosts a selective router, at least 72 hours at full office load?
b) Test and maintain all backup power equipment in such central offices in accordance with the manufacturer's specifications?
c) Design backup generators in such central offices for fully automatic operation and for ease of manual operation, when required?
d) Design, install, and maintain each generator in any central office that is served by more than one backup generator as a stand-alone unit that does not depend on the operation of another generator for proper functioning?

□ Yes for all central offices. Please fill in the report which lists all central offices meeting all backup power requirements, i.e., meeting a), b), c) and d).

□ Yes for some central offices but alternative measures for other central offices. Please fill in the report which lists all central offices meeting all backup power requirements, i.e., meeting a), b), c) and d). For each central office with alternative measures implemented, please provide those alternative measures using the "Alternative Measures for Backup Power for Central Offices" report.

□ No, but alternative measures for all central offices that directly serve a PSAP or host a selective router. For each central office with alternative measures implemented, please provide those alternative measures using the "Alternative Measures for Backup Power for Central Offices" report.

□ No. Please explain:

□ Not applicable. Please explain:

Alternative Measures for Central Office Backup Power

Central Office – CLLI code (fill in CLLI code):

State (chose from menu):
- AK
- AL
- AR
- CA

Central Office Contains a Selective Router:
- Yes
- No

Has 72 Hours Back-Up (If SR) or 24 hours (If not SR, chose from menu)
- Yes
- Alternate Measures
- No

Alternates for Amount of Back-up Power (chose from menu):
- Alternative Measure 1
- Alternative Measure 2
- Alternative Measure 3
- Alternative Measure 4
- Alternative Measure 5
- Other

If "Other" is selected above, Please provide a description:

Certification Form Examples

(Under OMB Review; May Be Subject to Change)

Network Monitoring

Within the past year, has the certifying entity:

a) Conducted diversity audits of the aggregation points that it uses to gather network monitoring data in each 911 service area?
b) Conducted diversity audits of monitoring links between aggregation points and network operations centers (NOCs) for each 911 service area in which it operates?
c) Implemented physically diverse aggregation points for network monitoring data in each 911 service area and physically diverse monitoring links from such aggregation points to at least one NOC?

□ Yes for all 911 Service Areas. Please fill in the report which lists all the 911 service areas meeting network monitoring requirements, i.e., meeting a), b), and c).

□ Yes for some 911 service areas but alternative measures for other 911 service areas. Please fill in the report which lists all 911 service areas meeting network monitoring requirements, i.e., meeting a), b), c) and d). For each 911 service area with alternative measures implemented, please provide those alternative measures using the "Alternative Measures for Network Monitoring" report.

□ No, but alternative measures for all 911 service areas. For each 911 service area with alternative measures implemented, please provide those alternative measures using the "Alternative Measures for Network Monitoring" report.

□ No. Please explain:

□ Not applicable. Please explain:

Alternative Measures for Network Monitoring

911 Service Area:

Alternative measure for network monitoring (chose from menu):

- Alternative Measure 1
- Alternative Measure 2
- Alternative Measure 3
- Other

If "Other" is Selected Above, Please Provide an Explanation of Other Alternative Measure:

Break for Questions

- Certification process and data entry:
  - John Healy
    Associate Division Chief
    Cybersecurity and Communications Reliability Division
    (202) 418-2448
    john.healy@fcc.gov

PSHSB Staff Contacts

- *Report and Order* and rules:
  - Eric Schmidt
    Attorney Advisor
    Cybersecurity and Communications Reliability Division
    (202) 418-1214
    eric.schmidt@fcc.gov
- Certification process and data entry:
  - John Healy
    Associate Division Chief
    Cybersecurity and Communications Reliability Division
    (202) 418-2448
    john.healy@fcc.gov