The "State of 911" Webinar Series

National 911 Program
May 7, 2014
12:00 PM EDT

911.gov

- The National 911 Program designed this webinar series to provide a unique combination of useful tools, information about Federal and State participation in the NG911 process, and real experiences from early adopters about the NG911 transition process underway in regions around the country

- Webinars will be held bimonthly and consist of presentations from a Federal-level 911 stakeholder and state-level 911 stakeholder, each followed by a 10 minute question and answer period

- For more information on future events, past webinar recordings and presentations, and to learn more about the National 911 Program, please visit www.911.gov

"State of 911" Webinar Series

911.gov

Agenda

- 12:00 – 12:20 PM
  - Alex Kreilein, Technology Policy Strategist, DHS Office of Emergency Communications
    - Cybersecurity and NG911
- 12:20 – 12:30 PM
  - Q&A
- 12:30 – 12:50 PM
  - Lynn Questell, Executive Director, Tennessee Emergency Communications Board
    - Best practices/lessons learned in deploying a statewide NG911 network
- 12:50 – 1:00 PM
  - Q&A

Cyber and Physical Threat and Risk Analysis to Improve the NPSBN (CAPTAIN)

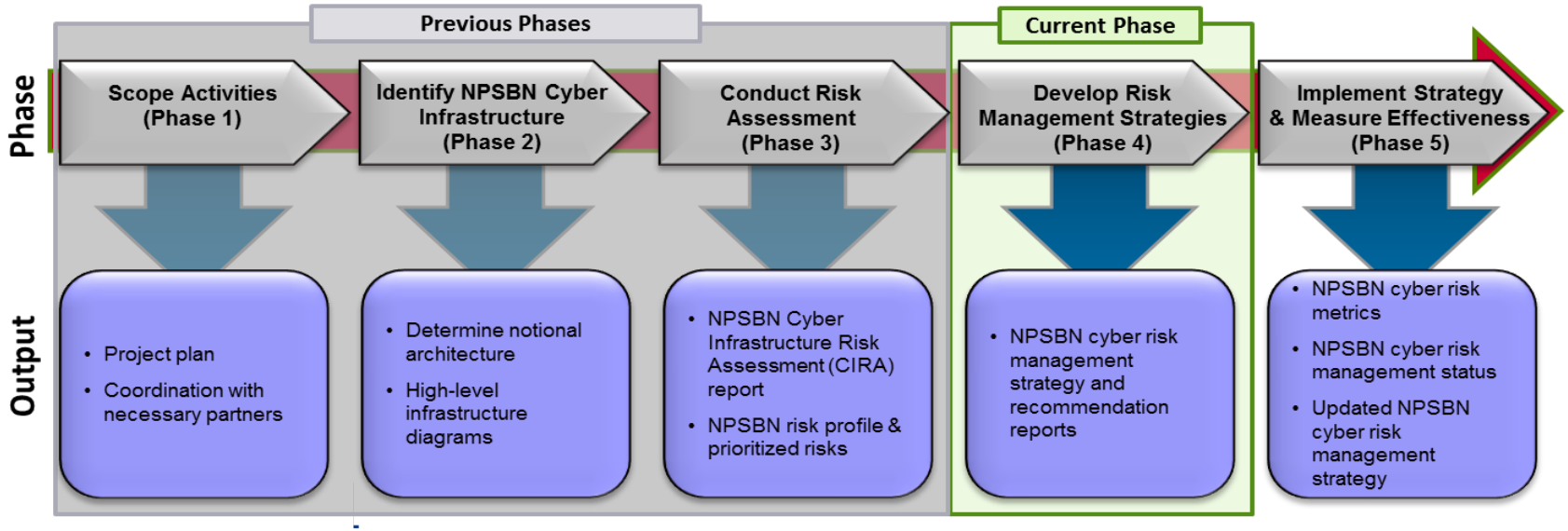
State of 911 Webinar Discussion

May 7, 2014

Homeland Security

What is the CAPTAIN Program?

- The Cyber and Physical Threat and Risk Analysis to Improve the NPSBN (CAPTAIN) Program is an ongoing Department of Homeland Security (DHS) effort to evaluate and mitigate risks to the cyber infrastructure of the Nationwide Public Safety Broadband Network (NPSBN)
  - Part of DHS' leadership role in assessing cyber risks to civilian agencies and protecting the Nation's critical infrastructure
  - Focused on nationally significant risks; not specific to individual networks, systems, providers, or geographic regions
- Proactive effort intended to better inform nationwide policies, priorities and risk mitigation efforts
  - Will be provided to national-level governance bodies, such as the First Responder Network Authority (FirstNet) and the Federal Communications Commission (FCC)



What are the cyber risks in the NPSBN?

- Broadband technologies may introduce new risks that the public safety community has not had to address in the LMR environment
  - Networks are not privately owned, yet must remain operable and interoperable at all times, especially during disaster scenarios
  - Mobile cyber threats unique to public safety are not well understood
  - Data on the NPSBN could be high-value target for hackers, criminals, and terrorists
- Sensitive data transmitted through the NPSBN will need to be properly safeguarded
  - Sensitive personal information, such as criminal and medical records
  - Critical infrastructure information
  - Sensitive investigative or operational information
- Interconnection with other public safety systems like NG911 will create additional vulnerabilities
- Trust in the NPSBN must be maintained for it be successful due to public safety's critical missions and sensitive information that it will support




Homeland Security

How does DHS define "cyber risk?"

- "Cyber risks" are anything that would negatively impact the **security** and **resiliency** of the cyber infrastructure
  - **Cyber security** refers to the *confidentiality, integrity,* and *availability* of the data
  - **Resiliency** refers to the ability of the infrastructure to maintain continuous operability
- Key risk terms:
  - **Threat:** natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
  - **Vulnerability:** physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard
  - **Likelihood**—chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities
  - **Consequence**: effect of an event, incident, or occurrence

Risk = the ***likelihood*** of a threat exploiting a vulnerability and the potential ***consequence*** or impact of that event

Source: DHS Risk Lexicon. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

Homeland Security

How did the CAPTAIN Program assess risks and what did it find?

- CAPTAIN program performed a cyber infrastructure risk assessment of the NPSBN in 2012 and 2013
  - Defined four attributes that are critical to ensuring the success of the NPSBN: **operability**, **interoperability**, **cybersecurity**, and **resiliency**
  - Identified 117 overall risks that would cause the loss or degradation of one or more of those four attributes; of these, identified 32 high-priority risks, with higher likelihoods of occurrence and a greater potential consequences
- Of the four attributes listed above, **cybersecurity** had the highest number of high-priority risks
- Three categories contain a significant amount of high-priority risks
  - **Governance, Policy, and Planning**
    - Minimal policies, standards, and guidance has been issued to date; critical need for a wide range of attributes, including all of the network attributes studied by the CIRA
  - **Networks, Systems, and Services**
    - Critical data at risk from malware and malicious attacks on applications and databases; operability and availability of networks threatened by unintentional planning oversight and misconfiguration
  - **Physical Infrastructure**
    - Operability, continuity, and security of infrastructure face significant threat from natural disasters and unintentional threats such as failures in planning, maintenance, and testing

What are the potential cyber risks to NG911?

- Most of the risks to the NPSBN apply to NG911, but the risks may be higher because of the public-facing nature of PSAPs
  - Whereas the NPSBN is a closed system available only to authorized users, NG911 services will connect directly to the public meaning that there will be more “touch points” to serve as potential vulnerabilities
  - GAO states that there are more than 6,000 PSAPs that answer 24 million calls nationwide[1]
- Specific cyber risks to NG911 and PSAPs include:
- Threat actors using malicious code or software; GAO report describes several
  - Spammers, phishers, and criminal groups looking to commit identity theft and fraud
  - Hackers seeking thrills or forms of activism
  - Corrupt or disgruntled insiders
- Denial of service attacks
  - Potentially more severe over IP-based communications networks because denial-of-service can be made more forceful through automation and geographic dispersion
  - Enables perpetrators to more easily hide their identities
- Wiretapping and traffic hijacking
  - IP traffic open to more exploitation and diversion than analog voice traffic
  - Easier to hijack or eavesdrop anonymously

[1]http://www.gao.gov/assets/670/660404.pdf

Homeland Security

How will the NPSBN and NG911 interconnect and what are the potential vulnerabilities?

- Traffic between PSAP and NPSBN users will be sent through a mix of networks, including both government- and commercial-owned networks
  - Less ability to control and secure traffic
  - No clear lines of end-to-end responsibility
  - Increased number of connections between systems brings greater potential for loss of network if any go down
- Dispatch operations will connect to responders through NPSBN
  - Potential transfer of sensitive information, including details about caller (medical, location), geospatial emergency and originating call location data
- Interconnection of databases across numerous first responder enterprises
  - Containing highly sensitive information about individuals (medical, legal records) and critical infrastructure
- Emergency responses will require significant interconnection between PSAPs and NPSBN
  - Greater number of interconnections means that there are more potential physical risks that could bring down the resiliency of the networks

Homeland Security

What are the next steps?

- CAPTAIN to deliver report soon to FirstNet with strategies to mitigate high-priority risks to NPSBN
- Next phase of CAPTAIN will look at strategies for State and local entities to mitigate cyber risks to their portions of the NPSBN and the systems with which they interconnect
  - Opportunity to examine connections between PSAPs and NPSBN at State and local levels
  - Opportunity for NG911 to provide feedback and shape recommendations
- As NPSBN and NG911 continue implementation and evolution, future opportunities will exist to examine shared infrastructure, connections, and cyber risks

Homeland Security

Back-Up Slides: High-Priority Risks

Homeland Security

High-Priority Risk Details: Cybersecurity

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Non-Standard Authentication	The unclear or inconsistent administration and coordination of authentication, access control, and identity credentials lead to users being unable to connect to the RAN or Core or maintain their connection when roaming	RAN & Core	Unintentional	**Medium**	**Medium**	• Users from one jurisdiction not able to connect in another because they don't have proper credentials
Security Policies	A malicious threat actor exploits RAN network infrastructure, data, or users because of a lack of or poorly defined security policies, requirements, or standards	RAN	Deliberate	**High**	**High**	• Network has many vulnerabilities that can be exploited by malicious actors
Malware (RAN)	A malicious threat actor uses malware to exploit the network infrastructure, systems, or applications on the RAN	RAN	Deliberate	**High**	**High**	• Malware embedded in hardware, software, applications • Viruses, worms and hijack attempts damage infrastructure • Malicious applications (e.g., keyloggers) steal data • Spear-phishing attack gets data from PS official
Database Attack or Exploitation	A malicious threat actor exploits database services in the Core	Core	Deliberate	**Medium**	**High**	• Man-in-the-middle attack allows hacker to gain entry into sensitive data • Open-source database hacking tools used to find vulnerabilities • SQL injections • By exploiting vulnerabilities in connected systems or databases, a hacker might get into one database or system and obtain access to others

High-Priority Risk Details: Cybersecurity continued

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Database Failure or Misconfiguration	An unintentional threat (failure or misconfiguration) limits the availability of database services	Core	Unintentional	Medium	High	• Programming failures, software design defects, inaccurate modification result in accidental deletion of data
Malware (Core)	A malicious threat actor uses malware to exploit network infrastructure in the Core	Core	Deliberate	Medium	High	• Malware embedded in hardware, software, applications • Viruses, worms and hijack attempts damage infrastructure • Malicious applications (e.g., keyloggers) steal data • Spear-phishing attack gets data from PS official
End Point & User Devices	A malicious threat actor exploits security vulnerabilities in end point devices	RAN	Deliberate	Medium	High	• Theft of a device (smartphone, laptop, tablet, etc.) enables exploitation of the content, possibly through accessing hard drive or possibly through the device's interface if no or weak password protection and/or encryption

High-Priority Risk Details: Network Management and Training

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Network Management Policies	An unintentional threat damages the operability of the RAN because of inadequate network management practices resulting from a lack of or poorly defined policies or requirements	RAN	Unintentional	**Medium**	**High**	• One jurisdiction's failure to maintain or update its infrastructure or systems causes problems for responders who roam onto network or provides a back door vulnerability for a larger cyber attack
Security Training	A malicious threat actor exploits RAN infrastructure because users, administrators and operators receive no or ineffective training on proper usage, security practices, and maintenance requirements	RAN	Unintentional	**Medium**	**High**	• Responders make mistakes that could be easily avoided and damage the network • Users do not know how to prevent incidents • When incidents occur, users do not how to handle or who to inform
Network Management Enforcement	The operability of the RAN suffers damage because inadequate enforcement of network management policies causes ineffective or inconsistent practices among system operators and administrators	RAN	Unintentional	**Medium**	**Medium**	• One jurisdiction's failure to maintain or update its infrastructure or systems causes problems for responders who roam onto network or provides a back door vulnerability for a larger cyber attack
Operations Training	Unintentional threats damage the operability of the RAN because users, administrators and operators receive no or ineffective training on proper usage, security practices, and maintenance requirements	RAN	Unintentional	**Medium**	**Medium**	• Avoidable mistakes are made that damage the network • When incidents occur, users do not how to handle or who to inform
End of Lifecycle	An unintentional threat damages the operability of the RAN because infrastructure is at the end of its lifecycle is not properly maintained or replaced	RAN	Unintentional	**Medium**	**Medium**	• Equipment failure occurs that could have been prevented • Potential lack of parts for specialized equipment when it fails

High-Priority Risk Details: Infrastructure Resiliency

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Vulnerable Location (RAN)	A natural threat damages or destroys RAN infrastructure located in vulnerable facilities or locations	RAN	Natural	High	Medium	• Natural disaster (e.g., hurricanes, flooding, high winds, earthquakes) damage or destroy network segments
Resiliency (Natural Disasters)	A natural threat damages or destroys RAN infrastructure that lack preventive measures to ensure resiliency (such as diverse and redundant communications paths and conduits)	RAN	Natural	High	Medium	• Single points of failure disrupted by high winds or winter weather conditions (e.g., aerial backhaul lines, antennas) • Equipment failures from inclement weather
Resiliency Policies	An unintentional threat damages the operability of the RAN because a lack of or ineffective policies, guidance, or requirements to ensure adequate resiliency measures	RAN	Unintentional	Medium	High	• No resiliency measures built into network because not required • Resiliency measures are ineffective because there is not proper guidance or policies to follow
Vulnerable Location (Core)	A natural threat damages or destroys Core infrastructure located in vulnerable facilities or locations	Core	Natural	Medium	High	• Natural disaster (e.g., hurricanes, flooding, high winds, earthquakes) damage or destroy network infrastructure
HVAC	A natural threat damages or destroys RAN infrastructure due to inadequate power, heating, ventilation, and air conditioning (HVAC) systems within infrastructure facilities	RAN	Natural	Medium	Medium	• Insufficient cooling / cooling system failure • Lack of back-up power / power system single point of failure
Resiliency (Unintentional Threats)	The operability of the RAN suffers because an unintentional threat exploits the lack of resiliency measures (such as diverse and redundant communications paths and conduits)	RAN	Unintentional	Medium	Medium	• Single points of failure disrupted by accidents or construction (e.g., aerial backhaul lines, antennas) • Equipment failures • Design limitations hamper operability

High-Priority Risk Details: Incident Detection and Response

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Incident Response and Help Desk (Unintentional Threat)	An unintentional threat (e.g. accident or mistake) damages the operability of the RAN and Core networks because of the lack of or ineffective incident detection and response policies and governance (including help desk support)	RAN & Core	Unintentional	**Medium**	**High**	• Response procedures not coordinated across disparate vendors and service provider networks, leading to inability to resolve widespread outages or network issues
Incident Response and Help Desk (Deliberate Threat)	A malicious threat actor exploits vulnerabilities in the RAN or Core because of a lack of or ineffective incident detection and response policies and governance	RAN & Core	Deliberate	**Medium**	• High	• If a vulnerability is exploited, it goes unnoticed (e.g., a hacker gets into a database) • No clear lines of delineated authority
Personnel Access	Personnel needed to restore systems or networks after an outage cannot obtain proper access and credentials because of a lack of or ineffective planning	RAN	Unintentional	**Medium**	**High**	• As technicians and additional telecom support is needed to restore service, they are denied timely access because of credentials needed to get on site
Network Outage Response	Services in the RAN or Core cannot be restored after an outage because of a lack of or ineffective network outage response policies and planning	RAN & Core	Unintentional	**Medium**	**High**	• Response procedures not coordinated across disparate vendors and service provider networks, leading to inability to resolve widespread outages or network issues

High-Priority Risk Details: System Planning and Coordination

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Coordination with Partners	Unintentional network overload damages the operability of the RAN because the lack of or ineffective coordination and planning with key partners (e.g., mutual aid agreements with neighboring jurisdictions, service level agreements with service providers) results in ineffective network design or hampers ability to respond to network incidents	RAN & Core	Unintentional	**Medium**	**High**	• Different segments of the network are built to different specifications, leading to inability to handle traffic spikes or clear lines of who should respond to an incident
Capacity Planning (Within Jurisdiction)	Unintentional network overload damages the operability of the RAN because of ineffective capacity planning and/or system implementation	RAN	Unintentional	**Medium**	**High**	• Network falters under the increased usage load of an emergency response situation
LTE Prioritization	Unclear or inconsistent administration and coordination of priority services implementation leads to users being unable to connect to the RAN or maintain their connection and quality of service when roaming	RAN & Core	Unintentional	**Medium**	**High**	• Responder has priority on one part of the network, roams to the next jurisdiction and
Capacity Planning (Inter- Jurisdiction)	Unclear or inconsistent administration and coordination of capacity and architecture planning leads to users being unable to connect to the RAN or maintain their connection and quality of service when roaming	RAN	Unintentional	**Medium**	**High**	• Network could be vulnerable to overload when resources are strained, such as during a large event response or when damage to a portion of the RAN prompts multiple user types to utilize common architecture
Interoperability Standards & Enforcement	The lack of or ineffective testing, implementation and enforcement of interoperability standards and requirements lead to devices being unable to connect to the RAN or maintain their connection and quality of service when roaming	RAN	Unintentional	**Medium**	**High**	• Unanticipated incompatibility issues arise when network is needed

High-Priority Risk Details: Back-Up Capabilities

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Back-up Failure due to Natural Disaster (RAN)	A natural threat disrupts the continuity of the RAN because back-up capabilities, systems, or infrastructure are not regularly tested, inspected, or maintained	RAN	Natural	High	High	• Inability to switch (manually or physically) to COOP/COG systems when needed • Additional downtime needed to fix system
Back-up Failure due to Natural Disaster (Core)	A natural threat disrupts the continuity of the Core because back-up capabilities, systems, or infrastructure are not regularly tested, inspected, or maintained	Core	Natural	Medium	High	• Carriers try to switch to back-ups that don't work because they weren't properly tested • Inability to switch (manually or physically) to COOP/COG systems when needed • Additional downtime needed to fix system
Redundancy & Failover	A natural threat disrupts the continuity of the RAN because of a lack of or ineffective infrastructure redundancy, back-up, or failover capabilities	RAN	Natural	Medium	High	• If no redundancy, single points-of-failure able to bring down service in inclement weather conditions (wind, winter, flooding, heat, etc.) • No back-up or failover is self-explanatory
Back-up Failure due to Unintentional Threat (RAN)	A threat disrupts the continuity of the RAN because back-up capabilities, systems, or infrastructure are not regularly tested, inspected, or maintained	RAN	Unintentional	Medium	High	• Carriers try to switch to back-ups that don't work because they weren't properly tested • Inability to switch (manually or physically) to COOP/COG systems when needed • Additional downtime needed to fix system

Please use the “Raise Hand” feature to ask a question.

Questions

Next Generation 911 Deployment & Funding

Lynn Questell
Executive Director
Tennessee Emergency Communications Board

May 2014

Tennessee Emergency Communications Board (TECB)

- The Tennessee Emergency Communications Board (TECB) was created in 1998 to assist Tennessee's 100 emergency communications districts in the areas of management, operations and accountability, and to establish emergency communications for all citizens of the State.

- By law, 5 of the Board's 9 members have experience in 911; in fact, all 5 run 911 PSAPs.

What Does the TECB Do?

- Administers statewide deployment of 911 service, including Phase II & the Next Generation 911 Project
- Provides funding, technical and operational assistance and oversight to Emergency Communication Districts
- Sets technical standards for PSAPs
- Administers dispatcher training requirements

Milestones in 911 Deployment in Tennessee

- Tennessee was the 3rd State to Provide Statewide Enhanced 911 Phase 2 Service
- Received award as Best State or Regional Program by the E-911 Institute in 2005
- Deploying Next Generation 911 Project (NG911)

NG911 Funding in Tennessee

- The TECB is currently funded by a $1.00/user/month fee on all non-wireline communications service capable of connecting to 911
- Local 911 also collected a 911 fee on landlines up to $1.50 for residential and $3 for businesses
- TN law allows revenue collected by TECB to remain in a separate, interest bearing account and the TECB began saving for NG911 in 2006
- The law required 25% of collections to be distributed locally; the TECB has distributed about 60% -- about $45.4 million in recurring funds -- and made available to each 911 district over $450,000 in non-recurring equipment funding

NG911 Funding in Tennessee

- Reductions in landline service and carriers impacted local 911 collections
- In 2014, the TN NENA, carriers and TECB joined in support of a revenue neutral bill that set the 911 fee on all telecommunications technology at a uniform rate of $1.16
- Under the new law, the TECB distributes to each 911 district “a base amount equal to the average of the total recurring annual revenue the district received from distributions from the board and from direct remittance of 911 surcharges for fiscal years 2010, 2011, and 2012; however, in no event shall such distribution be less than the amount the district received in 2012”
- The TECB will have about $16.5 million in recurring funds and $36 million in reserves to complete NG911

Pre-deployment Preparation for NG911

2006 NG911 Feasibility Study Completed

2006 Passage of Law Authorizing TECB to Deploy NG911

2006 TECB Starts Saving for NG911 Project

2008 TECB decides to use NetTN Network for NG911; AT&T is NetTN's vendor

2010 General Assembly Committee Approves NetTN Contract Amendment Adding Initial NG911 Terms

2010 RFP for 911 Management Released

2011 TCS awarded contract for Management of 911 Aspects of NG911, NOC, ALI Database

NG911 Objectives

- Improved Reliability, Redundancy & Repair
- Statewide Call Transfer and Failover Capabilities
- Improved Communications Between PSAPs
- Harassing NSI Calls Rerouted
- Text, Photos and Video to 911

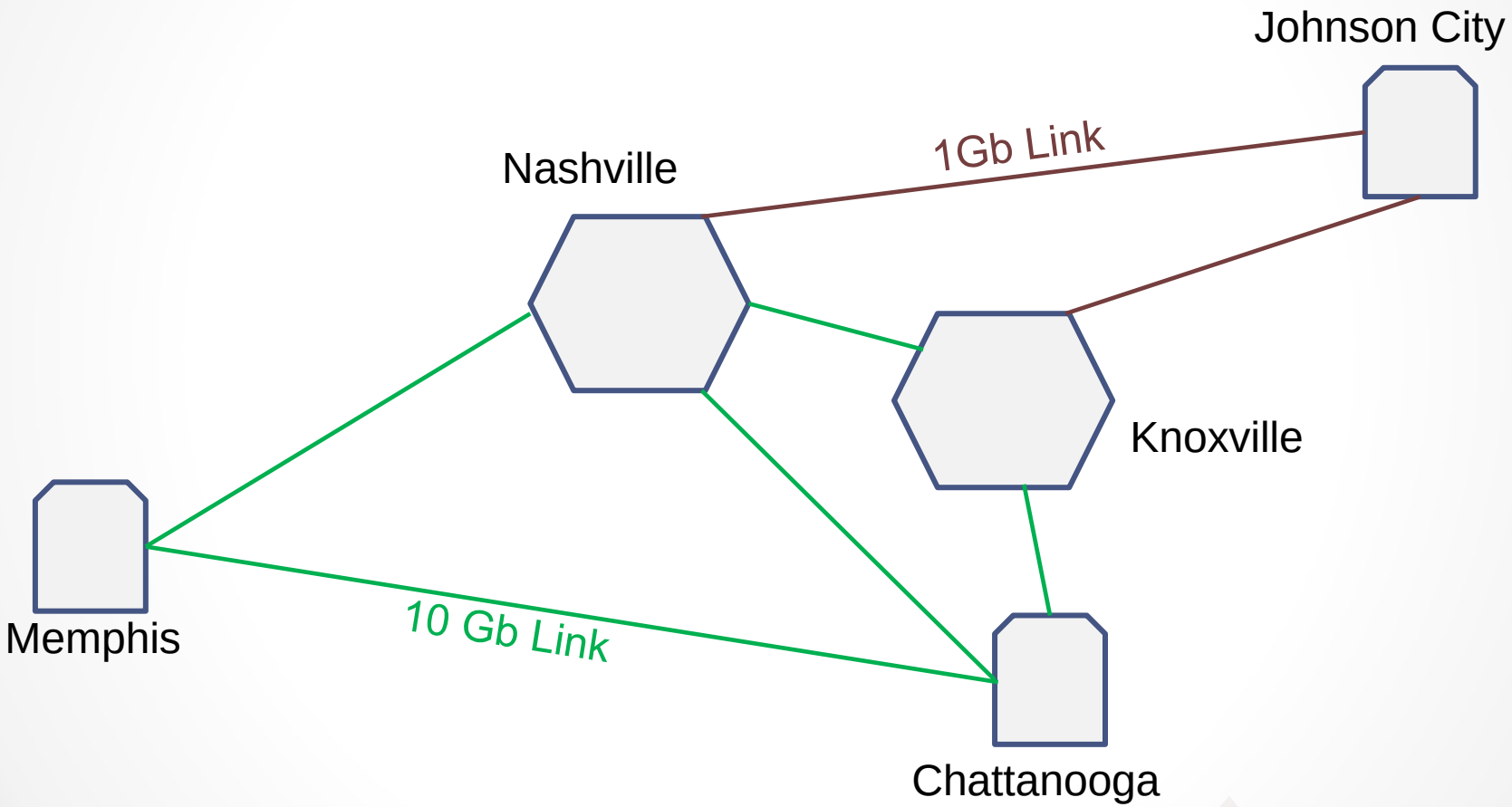
What is NG911 in TN?

- Tennessee's NG911 project runs on a private, secure, statewide Multiprotocol Label Switching (MPLS) network called "NetTN" managed by the TN Office of Information Resources: Tennessee's NG911 solution contains:
  - 2 fully redundant Network Control Centers to route calls
  - 4 wireless Network Aggregation Points, which are connected to the Control Centers via two separate routes
  - Each wireless carrier must connect to at least 2 aggregation points
  - Each PSAP must connect to the core
  - NENA i3 Compliant

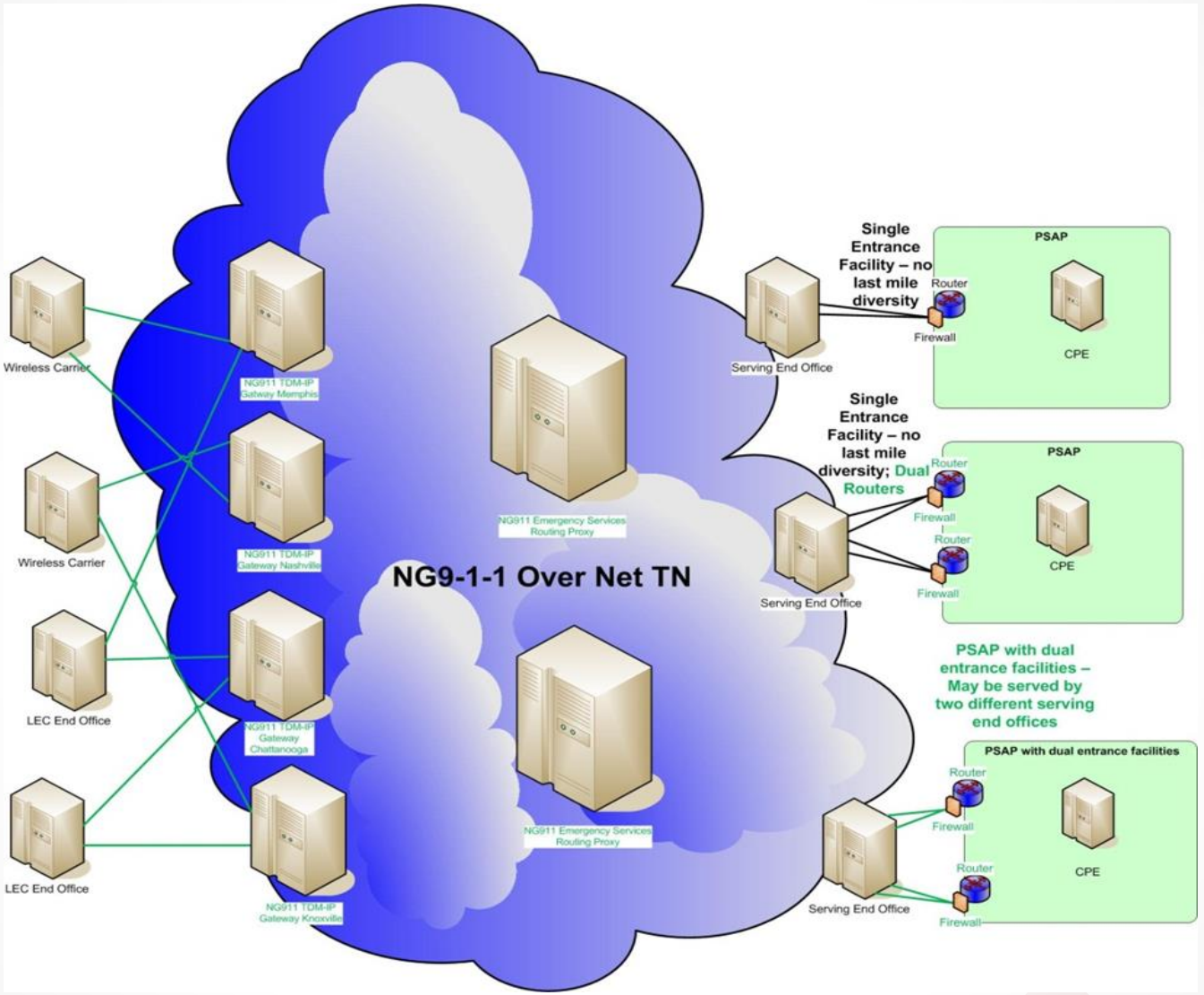
NET TN Core

- IP routing core with multiple logical VPNs
- 10 Gb Backbone
- 1 Gb Diverse Backbone to Johnson City
- Five 9’s core availability with world class service level agreements (ex: 3 hour time to repair per site)
- Up to 10 Gb client access with National remote access capability

Example of Network Design



NG911 Over NetTN



NG911 Deployment Plan

Stage 1: Deploy Core Network, including 2 redundant C/Os & 4 Aggregation Points; Connect all PSAPs and Wireless Carriers direct connecting to the core; Create a uniform, statewide GIS mapping system, focusing on ESN Boundaries, Centerlines and Address Points; Deploy NOC

Stage 2: Provide wireless call delivery to the PSAPs over Network

Stage 3: VoIP and Wireline deployment, ALI database deployment, Call Routing via Statewide ALI; Deploy NSI Diversion Process

NG911 Status Report

- The Core was deployed in September 2011, core testing completed in January 2012
- All CMRS (wireless) carriers direct connecting to the network completed their deployment by the end of 2013
- Network Operations Center operating 24x7x365

NG911 Status Report

- As of September 2013, 99% of PSAPs were at some stage of deployment
- All PSAPs have signed a user agreement setting out NG911 security requirements –no unauthorized network connectivity to internet
- Developing agreements to govern VoIP and Aggregator deployment and operation
- Statewide project to convert to uniform GIS standard and eliminate gaps and overlaps in ESNs completed – website deployed for updates

NG911 Status Report

- Of the 140 Sites to be on the network, 39% are accepting live wireless traffic over NG911 (Stage 2)
- As of March 2014, there is an overall average of the ALI to GIS Address point accuracy of 97%
- Administrative ALI is expected to be online by mid- 2014
- With the Admin ALI online, production of the statewide MSAG will be completed
- The first legacy Selective Router area (Jackson, TN) to go online Stage 3 (wire-line and VoIP traffic) will be complete by end of the year 2014

Roles of the Major Players

TECB	Purchaser and Manager of NG911 Website: http://www.tn.gov/emergency/index.shtml
OIR/NetTN Program Office	Oversees AT&T contracted statewide MPLS network
AT&T	Service provider for the state wide MPLS fiber network Service provider for the NextGen Selective Router (xSR) solution supporting NG911
TCS	Vendor for NG911 Managed Services, including deployment management, risk and change management, monitoring, ALI Database and 24x7x365 NOC
MCP	Technical consulting
OIR/GIS	GIS services

Questions or Comments?

THANKS FOR YOUR TIME

Please use the “Raise Hand” feature to ask a question.

Questions

- Thank you to all of today's presenters and participants and we look forward to seeing you at our next "State of 911" webinar

Tentative Date	Presenters	Registration
Wednesday, July 9, 2014	**TBD**	Registration will open June 9, 2014
Wednesday, September 10, 2014	**TBD**	Registration will open August 10, 2014

Future "State of 911" Webinars

911.gov

Contact Us

Laurie Flaherty
National 911 Program Coordinator
202-366-2705
laurie.flaherty@dot.gov

For questions regarding future webinars, please contact NG911wg@bah.com