Q1  What is Pierce County doing to prepare for Next Generation 911 (NG911) and the range of features and functions it provides to both the citizens and 911 call centers?

A1  The E911 Program Office is using the standards and information documents developed and published by the National Emergency Number Association (NENA) to guide its approach to preparing public safety answering points (PSAPs) for NG911 functionality.

Specifically, the program office is using the “NENA Detailed Functional and Interface Standards for the i3 Solution” (STA-010.2-2016) and “NENA Security for Next-Generation 911 Standard” (75-001) to establish the fundamental cyber security monitoring, reporting, and response features that will be in place for fully Internet Protocol (IP)-connected PSAPs.

These efforts ensure that all IP-based communications into the PSAP are inspected for malicious payloads that could compromise PSAP operations or personally identifiable information collected from callers.

As the State of Washington Emergency Services IP Network (ESInet) becomes capable of delivering new types of IP-based messages to PSAPs, these security features ensure that every data packet into and out of the PSAP does not contain a threat that could compromise the confidentiality, availability, or integrity of these digital communications.

Q2  What is the baseline for turning on security services, knowing that there will always be new threats?

A2  The E911 Program Office is in the final stages of a ‘Proof of Concept’ project with the developer of a Security Event and Information Monitor (SEIM) device. Once the concept of operations has been proven viable, the product will be implemented at each PSAP within Pierce County connecting to the State of Washington ESInet.

Q3  What is the PSAPs role and what is Pierce County’s role in activating text-to-911 at 911 call centers?

A3  The decision to implement text-to-911 remains in the hands of each PSAP. Once a PSAP has made the operational decision to implement and activate text-to-911 services, the E911 Program Office serves as the coordination point between the PSAP, the State of Washington ESInet, and the Wireless Service Providers (Cellular Carriers) in order to test and activate this service.

Q4  Are E911 Excise Tax funds supporting Joint Base Lewis-McChord and Washington State Patrol-Tacoma?

A4  Yes. State law requires that everyone that lives or works in Pierce County have access to 911 services. This includes the limited access state and federal highways as well as the over 90,000 individuals that live and work on JBLM.
Q5 How is the Pierce County E911 Program Office collaborating with 911 call centers; identifying and establishing best practices, and standards?

A5 E911 Program staff serve on several subcommittees of the State E911 Advisory Committee, including the 911 Communications Subcommittee, the Next Generation 911 subcommittee, and the Strategic Planning subcommittee. Other representatives of the E911 Program work on the GIS subcommittee and Public Education subcommittee. Through the work of these statewide committees, the best practices and standards are driven out to the actual operational practices here within the County.

The Pierce County E911 Program Office also hosts monthly meetings with representatives from JBLM, SS-911, and WSP-Tacoma where items of mutual concern are discussed and coordinated.

Additionally, using this collaborative model, the E911 Program Office is partnering with WSP-Tacoma to pilot the security monitoring and reporting that will be used as the standard for NG911 features and functions for all Pierce County PSAPs.

Q6 Which RCWs and WACs govern spending of the E911 Excise Tax funds?

A6 38.52.510 Statewide enhanced 911 services.
38.52.545 Priorities for enhanced 911 funding.
82.14B.030 County enhanced 911 excise tax on use of switched access lines and radio access lines authorized
118-66-020 Purpose and Priorities - establishes rules for expending 911 funds.
118-66-060 County Eligible expenses.
NEXT GENERATION 911 IMPLEMENTATION

Pierce County Emergency Management
Scott Heinze, Deputy Director
Jonathan Brock, E911 Coordinator
Hillman Mitchell, Cyber-Security Consultant
Today’s Presentation Objectives

• Overview of the E911 Program Office
• What is NG911?
• Why are we doing it?
• Where are we today?
• Where are we going in the short-term?
• Where are we going in the long-term?
• Questions
Who we are…

• Jonathan Brock, E911 Coordinator
  – Former 911 Program Coordinator for State of Oregon
  – Chair, 911 Communications Subcommittee (State E911 Advisory Cmte)
  – Member, NG911 Subcommittee, NG911 Strategic Planning Group, and NG-Security Standards working group
  – Degree in Computer Network Engineering

• Hillman Mitchell, Cyber-Security Consultant
  – Critical Infrastructure Cyber Security Consultants, LLC
  – 30+ years experience in computer and information systems engineering
  – Provides services to 8 of 16 Critical Infrastructure Sectors
  – Focus on protecting Life-Safety, Life-Sustaining, and Quality of Life services
Pierce County E911 Program Office

- RCW 38.52.510 – Statewide enhanced 911 service;

Each county, singly or in combination with one or more adjacent counties, must implement a countywide or multicounty-wide enhanced 911 emergency services system so that enhanced 911 is available throughout the state.
What is NG911?

The NENA Summary Definition of NG911 --

NG911 is a system comprised of hardware, software, data and operational policies and procedures to:

• Provide standardized interfaces from call and message services
• Process all types of emergency calls including non-voice (multi-media messages)
• Acquire and integrate additional data useful to call routing and handling
• Deliver the calls/messages and data to the appropriate PSAPs and other appropriate emergency entities
• Support data and communications needs for coordinated incident response and management
• Provide a secure environment for emergency communications
What is NG911? (continued)

The building blocks required for NG911 are:

- Emergency Services IP Network (ESInet)
- International Standards Compliant IP Functions
- Internet Engineering Task Force-based IP protocol standards
- Databases and Data Management
- Security Infrastructure and Processes
- Human Processes and Operational Procedures
Why NG911?

The way people communicate has changed dramatically since implementing E911…

The current system isn’t able to take advantage of new technology.
Where are we today?

• Caller’s TN is used to query the ALI database
• ALI database returns Address
• Address is used to query MSAG database
• MSAG database returns PSAP information

• This system was designed for Landline calls
• Work-arounds were developed for Wireless and VoIP callers
• Call delivery networks are based on CAMA and/or SS7 Signaling technologies
• Cannot accommodate meta-data delivery or technological advancements
Where are we going?

- Location of caller is known at the time a 911 call is placed
- Location is validated against GIS data to determine appropriate PSAP routing
- NG911 designed to accommodate any type of ‘call’
- Call delivery network is based on delivery of IP-packets (fully digital architecture)
- Meta-data is embedded into the packets being delivered to the PSAPs
- Allows for information to be forwarded to first responders and other public safety organizations
Where are we going?

ESInet II (NG911 Phase 1)
- SECO is responsible for deploying the statewide ESInet in WA
- Transition from ESInet I to ESInet II is being coordinated between the State and County 911 Program Offices
- ESInet II is fully IP

Cut-over to ESInet II in Pierce County:
- Joint Base Lewis-McChord – July 17
- 35th Street Branch – July 19
- Fire Comm – July 24
- WSP-Tacoma – November 27
Where are we going?

Call Flow:
1. LIS location sent to ECRF
2. ECRF finds address point
3. ECRF determines PSAP for location
4. ECRF sends PSAP URI to the ESRP
Where are we going?

In a NENA i3 NG911 Network, there are hundreds of interdependent features and services. These are accomplished in partnership between the providers, network operators, State, County, and PSAP.

The Pierce County E911 Program Office is responsible to ensuring the PSAPs of Pierce County are capable of receiving and processing the data packets that will be delivered through the ESInet, in a safe, secure manner.
Cyber Security Standards

NIST
National Institute for Standards & Technology
Federal ‘Best Practices’ for cybersecurity

CJIS
Criminal Justice Information Systems
DOJ/FBI Information Security Standard

NENA
National Emergency Number Association
Collaboratively developed

WA State
State E911 Coordinator’s Office & E911 Advisory Committee

05/11/2018
Cyber Security Standards

- NIST Cybersecurity framework built on 5 fundamental functions:

- **Identify**: develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities
Cyber Security Standards

- NIST Cybersecurity framework built on 5 fundamental functions:
  - **Protect**: develop and implement appropriate safeguards to ensure delivery of critical services
Cyber Security Standards

• NIST Cybersecurity framework built on 5 fundamental functions:

• **Detect**: develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Cyber Security Standards

- NIST Cybersecurity framework built on 5 fundamental functions:

- **Respond**: develop and implement appropriate activities to take action regarding a detected cybersecurity incident
NIST Cybersecurity framework built on 5 fundamental functions:

• Recover: develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident
Where are we going in the short-term?

• Goals for Implementation of NG911 Features & Services
  – Architect security and resiliency into the network
  – Ensure data can be forwarded safely
  – Ensure network uses Open Standards
Cyber Security Threat Landscape
Cyber Security Threat Landscape

• Understanding the threats and vulnerabilities is key to operating a reliable 911 system.

Confidentiality
Integrity
Availability

Global damage from ransomware attacks by 2019
146 Days

Cyber Attacks on Public Safety & Local Government: 184 (past 24 mo.)
### Why Security Matters

- **Goals for Implementation of NG911 Features & Services**
  - Architect security and resiliency into the network
  - Ensure data can be forwarded safely
  - Ensure network uses Open Standards

- **No chance for ‘Do Overs’**
Where are we going in the long-term?

<table>
<thead>
<tr>
<th>Washington State Patrol (D1)</th>
<th>Joint Base Lewis McChord</th>
<th>South Sound 911</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pilot project to prove security architecture and monitoring</td>
<td>Incorporate lesson’s learned at WSP</td>
<td>Available to assist and coordinate SS-911’s projects</td>
</tr>
<tr>
<td>Working with vendors to challenge conventional thinking and practices</td>
<td>System upgrades to receive digital network traffic</td>
<td>SS-911 holds the responsibility to implement NG911 within their center</td>
</tr>
<tr>
<td>Text-to-911 will be integrated into 911 equipment vs. using a separate, web-based system (Originally Puyallup)</td>
<td>Implementation will use an integrated solution to optimize call processing workflow</td>
<td></td>
</tr>
</tbody>
</table>

- Sharing lessons learned across the state and region to create success for others
- **Expand security practices to other critical infrastructure across the region** – through the Regional Coordinating Council and a Cyber Incident Response Team
Counties with Text-to-911

- 11 of 39 counties have implemented a Text-to-911 solution (data as of 09/2017)
- 9 of those counties are web-based with a single PSAP
- Web-based solutions require changes in call processing and workflow due to need for additional computer workstations with Internet connectivity
Counties with Text-to-911

- Grant & Snohomish Counties have deployed solutions integrated into their Viper systems
- Integrated solutions require additional network infrastructure to receive text messages
- Both counties have installed firewall devices that provide basic network protection for text messages

- PCEM is designing security for full NENA i3 functionality
Text-to-911 Implementation

- Public Education
- Wireless Coordination

Determine Solution
- Integrated
- Web-based

Equipment / Software Acquisition
- Coordinated with CPE vendor
- Cyber security

Policy / Procedures
- Response policies
- Transfer policies
- Staff training
Questions?
Scott Heinze,  
Emergency Management Deputy Director  
(253) 798-7143  
sheinze@co.pierce.wa.us

Jonathan Brock,  
Emergency Management E911 Coordinator  
(253) 798-2206  
jbrock@co.pierce.wa.us