Q-1  What do all those acronyms stand for?
A-1  *See comprehensive glossary at the bottom of this document

Q-2  What changes when we implement NG911 functionality?
A-2  From the call-maker’s perspective, there will be improved location information provided to the 911 Call Center. As a best practice, call-taker’s will still verify a caller’s location before dispatching resources. The next generation 911 (NG911) network supports a fully digital experience. This improved delivery network will allow for text, photos, videos, etc. to be delivered to the call-taker at the Public Safety Answering Point (PSAP) as well as forwarded to other public safety first responders.

Q-3  When I call 911 on my cell phone, how do they know my location currently? What will change when we go to Next Generation technology?
A-3  In today’s system, wireless location is provided using two different technologies determined by each wireless service provider. One technology uses the Global Positioning System (GPS) within the handset to determine its location. The other technology uses cellular tower triangulation to locate the handset.

With next generation 911 (NG911), the location will be imbedded in the digital communication stream between the call-maker and call-taker.

Q-4  Is Pierce County doing something different than the rest of the State when it comes to complying with NG911 requirements?
A-4  No. The entire 911 community within the State of Washington is using a standardized approach to implementing NG911 technologies. The State E911 Coordinator’s Office (SECO) is primarily responsible for the rollout of the new call delivery network that will be used to transport 911 calls to the PSAP. The County is, in turn, taking a deliberate and methodical approach to the cyber-security implementation for this new network.

Q-5  What is being done at the Federal level to address this [cyber-security] concern?
A-5  Nationally, there are several working groups within both the National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) establishing best practices for implementing cyber-security within a PSAP. These approaches are primarily focused on educating and training PSAP personnel.

The E911 Program Office is using the National Institute of Standards and Technology (NIST) cyber security framework to ensure that we can: Identify, Detect, Protect, Notify, and Recover from attacks.

Q-6  Can our 911 system be impacted by cyber-attacks even if they are not able to compromise the call processing equipment and data?
A-6  Yes. Coordinated cyber-attacks can flood the 911 network that calls will not be able to be delivered to the PSAP. Malicious software (malware) can be sent to cell phones that causes
them to automatically dial 911 over and over, effectively shutting down the 911 network – this is known as a Telephony Denial of Service attack.

Another type of attack floods the Internet with traffic specifically targeted at the servers that allow traffic to travel from a computer to a web site, effectively shutting down the Internet so that nothing can occur – this is known as a Distributed Denial of Service attack.

Q-7 Can our system be penetrated?
A-7 The SECO and Pierce County are being proactive in establishing cyber security procedures, processes, and systems to monitor, detect, and prevent malicious network traffic targeted at PSAPs. Without these in place, 911 centers could be taken offline or services disrupted, including compromising public safety information.

Q-8 Why did addresses on Key Peninsula have to change, was that because Pierce County purchased a system that wasn’t compatible?
A-8 No, Pierce County was out of compliance with Federal/National U.S. Postal standards. These standards are being adopted by PSAPs across the nation to allow for exchanging information seamlessly when 911 calls need to be transferred. The Key Peninsula re-addressing project was another step in ensuring that Pierce County’s addressing meets these standards.

Q-9 What would have happened if Pierce County decided not to change Key Peninsula addresses?
A-9 First responders may not be able to locate you when you call 911. In a catastrophic situation, 911 calls may not be able to be answered locally, historical incidents occurring within Pierce County have had first responders from neighboring counties respond to assist. Non-uniform addressing delays these life safety responses.

Q-10 How have the investments Pierce County and other agencies made to date improved the overall [communications] system?
A-10 The funding generated under Proposition 1 have allowed the County to upgrade the capacity and capabilities of the Single County-Wide Communications System (SCWCS). These improvements include both the communications system infrastructure and the equipment used by first responders. As an example, during the Amtrak derailment in December 2017, there were no responders that were unable to communicate with each other or dispatchers due to the system operating at capacity.

Additionally, the upgrades performed to the SCWCS allow for the latitude and longitude of portable radios to be transmitted to dispatchers when a first responder activates their Emergency Alert.

Q-11 What is Pierce County doing to meet the needs of Limited English Proficiency (LEP) users of 911?
A-11  The E911 Program Office funds a service known as Language line for use in PSAPs when callers are unable to speak English. Additionally, Emergency Management has worked to provide multi-lingual brochures for residents that speak other languages.

Q-12  Have you thought about a communication plan for how you inform the public about all of this information (the risks and what is being done to mitigate the risk)

A-12  We are currently working on a comprehensive refresh of the PCEM website, that will include significantly more information about the upcoming changes to the 911 system within the County. The State E911 Advisory Committee is also working on public education and outreach efforts through the Public Education subcommittee. We are always seeking new opportunities to share information about changes in technologies that affect public safety.

**Glossary:** (definitions provided in the order in which they appear in the PowerPoint presentation)

- HVAC – Heating/Ventilation/Air Conditioning system
- IT – Information Technology systems
- E911 – Enhanced 911 calling system
- CFS – Call(s) for Service
- VoIP – Voice over Internet Protocol (a telephone system that uses a computer network to connect a caller rather than the Public Switched Telephone Network)
- CPE – Customer Premise Equipment (such as 911 call processing equipment)
- GIS – Geographic Information Systems
- CAD – Computer Aided Dispatching system
- NG911 – Next Generation 911
- WSP – Washington State Patrol
- NENA – National Emergency Number Association
- APCO – Association of Public-Safety Communications Officials
- MSAG – Master Street Address Guide
- ALI – Automatic Location Information
- PSAP – Public Safety Answering Point
- NENA i3 PSAP – a Next Generation 911-enabled PSAP that can accept digital communications and data
- Ransomware – malicious software that encrypts data and disables a computer system until such time as a fee is paid to unlock the system
- NIST – National Institute for Standards and Technology
- CJIS – Criminal Justice Information Systems
- SECO – State E911 Coordinator’s Office, a division of the Washington Emergency Management Division
- PCEM – Pierce County Emergency Management
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?
CORNERSTONES OF A PSAP

- **Emergency Notification - Alert & Warning**
  - Emergency Broadcast System
  - Highway Advisory Radio
  - PC- ALERT / PC-WARN
  - Siren Systems

**E911 CFS Resolution & Disposition**

**911 CFS Incident Management & Stabilization**

**911 CFS Routed Proper PSAP**

**911 CFS Delivered to PSAP & Response determined**

**Public Safety Response**

**PSAP Activates Response Police, Fire, EMS**

**Radio System (Voice, Data & GIS)**


**911 Telephone System (CPE – Voice & Data/GIS)**

**Dispatching System (CAD/GIS)**

Emergency Networks GIS, CAD, Radio & Data Comms Systems

911 Network ESInet

Statewide Network, CPE, GIS, Service Providers

Statewide Network, CPE, GIS, Service Providers

Statewide Network, CPE, GIS, Service Providers

**CORNERSTONES OF A PSAP**

Emergency Networks GIS, CAD, Radio & Data Comms Systems

Service Providers GIS, Location Data

Service Providers Landline, Cell, VoIP

Emergency Networks GIS, CAD, Radio Systems

Emergency Networks GIS, CAD, Radio Systems

Emergency Networks GIS, CAD, Radio Systems

Emergency Networks GIS, CAD, Radio Systems

Emergency Services Communications System RCW 82.14B.020
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
• 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?

NG911 under ESInet II will enhance emergency services by creating a faster, more resilient system that allows digital information (voice, photos, video, text, and other data) to flow seamlessly from the public, through the 911 network, directly to first responders and others.

• Today, everything is data
• Increase location accuracy and the ability to accurately route calls
• New features and services are easier to ‘turn on’
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?
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

Cyber Attacks on Public Safety & Local Government: 184 (past 24 mo.)
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
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</td>
<td></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**
QUESTIONS?