Speakers

- **Greg Hauser** – North Carolina Emergency Management
  Communications Branch Manager/SWIC
- **Red Grasso** – North Carolina Department of IT
  Program Manager – First Responder Emerging Technologies Program
- **Pokey Harris** – North Carolina Department of IT
  Executive Director – North Carolina 911 Board
Agenda

• Identify the mission of Public Safety
• Identify what Public Safety Information is out there
• Identify measures to secure the information
Objective

- Provide attendees an alternative look at what public safety information is available for public consumption and how that information could potentially be used to do harm.

- The choice to secure information relies on the originator.
Disclaimer

• This presentation does not assume any entity or agency is doing anything incorrectly. Examples given are all North Carolina specific and are intended to show lessons learned.
State Interoperability Executive Committee (SIEC)
State Interoperability Executive Committee (SIEC)

<table>
<thead>
<tr>
<th>LOCAL REPRESENTATIVES</th>
<th>STATE REPRESENTATIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eastern Domestic Preparedness Regions</td>
<td>NC Office of the Governor</td>
</tr>
<tr>
<td>Central Domestic Preparedness Regions</td>
<td>NC Emergency Management</td>
</tr>
<tr>
<td>Western Domestic Preparedness Regions</td>
<td>Voice Interoperability Plan for Emergency Responders (VIPER)</td>
</tr>
<tr>
<td>Urban Area Security Initiative</td>
<td>NC 911 Board</td>
</tr>
<tr>
<td>NC Association of Rescue &amp; EMS</td>
<td>NC DIT: Broadband Infrastructure Office</td>
</tr>
<tr>
<td>NC Emergency Management Association</td>
<td>NC SPOC / FirstNet Project</td>
</tr>
<tr>
<td>NC Association of County Commissioners</td>
<td>NC Department of Transportation</td>
</tr>
<tr>
<td>NC League of Municipalities</td>
<td>NC Department of Health and Human Services</td>
</tr>
<tr>
<td>Association of Professional Communications Officers</td>
<td>NC Office of Emergency Medical Services</td>
</tr>
<tr>
<td>NC National Emergency Number Association</td>
<td>NC Homeland Security</td>
</tr>
<tr>
<td>NC Sheriff’s Association</td>
<td>NC Forest Service</td>
</tr>
<tr>
<td>NC Association of Chiefs of Police</td>
<td>North Carolina National Guard</td>
</tr>
<tr>
<td>NC Fire Chiefs Association</td>
<td>State Bureau of Investigation</td>
</tr>
<tr>
<td>Auxiliary Communications</td>
<td>Tribal Rep: Eastern Band of Cherokee Indians</td>
</tr>
</tbody>
</table>

Accurate as of 9/28/2020
North Carolina’s Public Safety Mission

- To ensure that citizens can access and receive assistance in their time of need.
- To protect day to day activities in accordance with all applicable laws.
Public Safety Vulnerabilities

• As a society we, the public, are connected to technology on a daily basis.
• How vulnerable are cellular voice and data networks?
• Is the information that the public has access to available to public safety?
Public Safety Vulnerabilities

• Public Safety Answering Points (PSAP)
  – The act of answering and processing a 911 call
  – Dispatching units to assist the public

• How does a PSAP ensure that their systems are safe and the information remains secure?
  – Hardware security (USB drives)
  – System security (Access to the Internet)
Public Safety Vulnerabilities

- NCDIT 911 Board Emergency Services IP Network
  - Network Monitoring and Assistance Center (NMAC)
- Security a Statewide 911 Network
  - 2800+ Telecommunicators acting as sensors
  - 2800+ Telecommunicators that could unwillingly do harm

Accurate as of 9/28/2020
North Carolina Emergency Management

North Carolina NextGen 911 - #NextGen911isNowGen911inNC
Emergency Services IP Network (ESINet) Status:

Live on ESINet
53
Active Projects
60
Approved for Migration
14

Accurate as of 9/28/2020
Information pathways within Public Safety

- **Email traffic** - Controlling who forwards the email
- **Radio traffic** – Controlling who is listening
- **Virtual traffic (WebEx, Teams, etc)** – Controlling who is watching

Accurate as of 9/28/2020
Information sharing vs. Information entitlement

- Information versus Data
- Who needs to know vs. who wants to know
  - Vertical Information Management
  - Horizontal/Lateral Information sharing
  - Responsible to take action
- Security and convenience
  - Keys and codes, access considerations

Accurate as of 9/28/2020
Public Information Availability

Is the information that public safety has access to available to the public?

• **Yes**
  Whatever we want to share
• **Good** (on purpose)
• **Bad** (mistake or on purpose)

Accurate as of 9/28/2020
Public Information Availability

Is the information that public safety has access to available to the public?

- No, but yes

People trying to circumvent a process to get the info.

Accurate as of 9/28/2020
Radio Traffic Interception

• Using free applications and web based platforms, sensitive, law enforcement information is being captured and used to the detriment of public safety.
  – Recent civil unrest activities
    • Charlotte, Raleigh, Asheville, Fayetteville, Greenville, etc.
• All agencies reported bad actors listening to smartphone apps for which law enforcement was broadcasting tactical movements.

Accurate as of 9/28/2020
Actions and options

North Carolina Emergency Management Communications Branch

Informational Bulletin
TLP: AMBER – Limited Disclosure

Date: May 31, 2020
To: Public Safety Stakeholders
From: NC EM • Communications Branch
Re: Online public safety scanner applications

Over the last two (2) days, the Communications Branch (ESF2) has received information regarding the use of online public safety scanner applications by members of the public to monitor law enforcement activities and tactical movements. There are numerous paid and free applications that allow for this to happen. Here is a quick rundown of what is happening and courses of action. ASSUME ALL RADIO TRAFFIC IS BEING MONITORED.

The radio traffic online originates from a member of the public who has connected a scanner to their computer. They provide this feed to the online provider. Since most law enforcement frequencies and talkgroups are un-encrypted (clear transmissions) the traffic, if it can be monitored, is fair game. Regardless of frequency, system characteristics, VIPER, local systems, etc., someone can listen and put it on the internet.

The NC Emergency Communications Branch (NC EM) recommends the following:

1. Locate the individual providing the online feed and request that they take the feed down temporarily.
2. Have your intel/PIO groups monitor your own online radio traffic to see what is actually out there.
3. Reach out to your local Emergency Management Coordinator. You may have someone locally who is trained to create communications plans and help with options. If you don’t that coordinator can find out where to get one.
4. Consider switching to side channels that normal scanner enthusiasts may not be tempted to put in their scanner. Public works, training channels, school security, etc. Something that doesn’t draw attention for enthusiasts.
5. Use encrypted talkgroups (see below for further). NOTE: If you or the PSAP patches a non-encrypted talkgroup to an encrypted talkgroup, the encryption goes away!
6. Use simplex (radio to radio) frequencies. There are options that should be programmed in your radio. Examples are ITACSII, VTAC1, VTAC9D, etc. You also may have

Accurate as of 9/28/2020
Questions?

THANK YOU!

WITHOUT COMMS...

YOU'RE JUST CAMPING

INTD  COMT  AUXCOMM

TERT  COML