Information and Process Security:
Public Safety Implications

2020 N.C. Cybersecurity Awareness Symposium

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

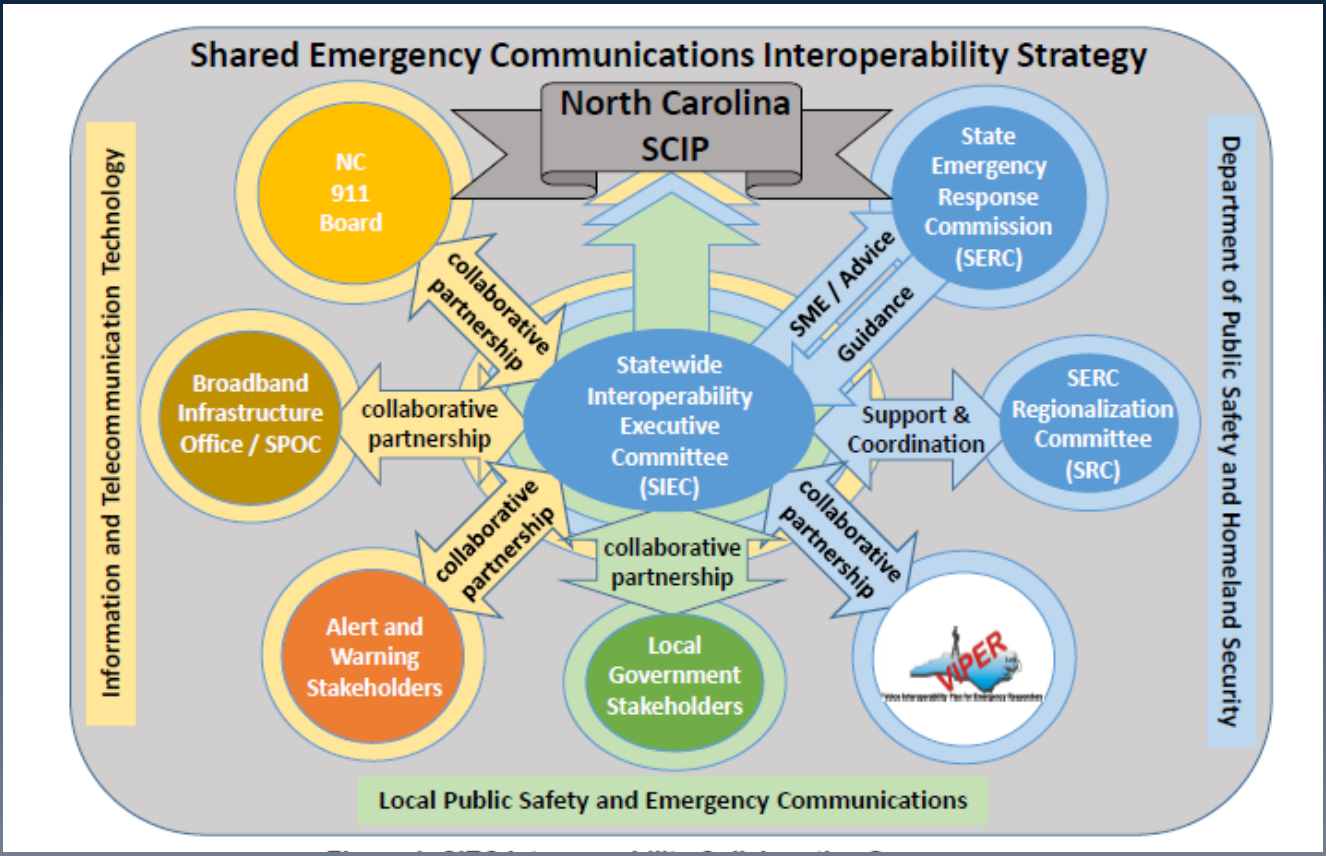
- Provide attendees an alternative look at what public safety information is available for public consumption and how that information could potentially be used to do harm.

- 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)



Accurate as of 9/28/2020

State Interoperability Executive Committee (SIEC)

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

Accurate as of 9/28/2020

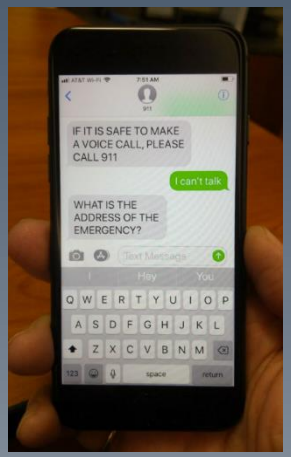
North Carolina's Public Safety Mission

- 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

Need for assistance is recognized

- 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 is accessed (voice or text)

- 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

Public safety is accessed (voice or text)

- 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

Last update: a minute ago

Active Projects

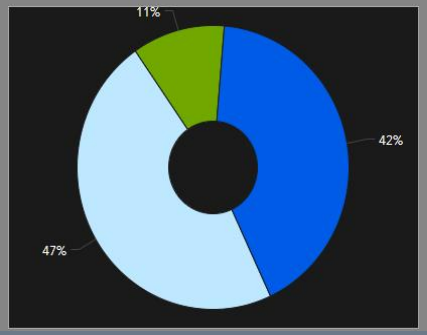
60

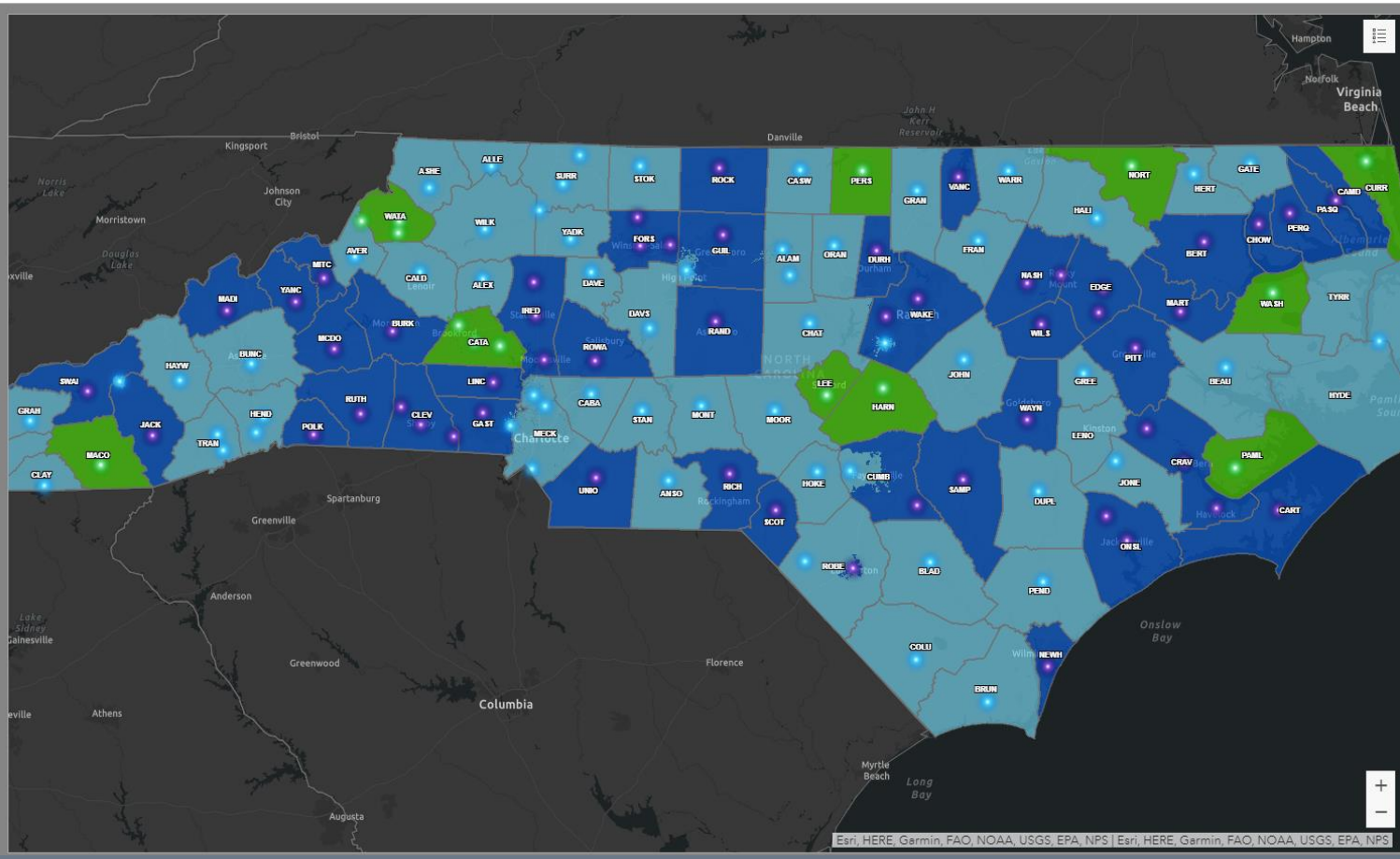
Last update: a minute ago

Approved for Migration

14

Last update: a minute ago



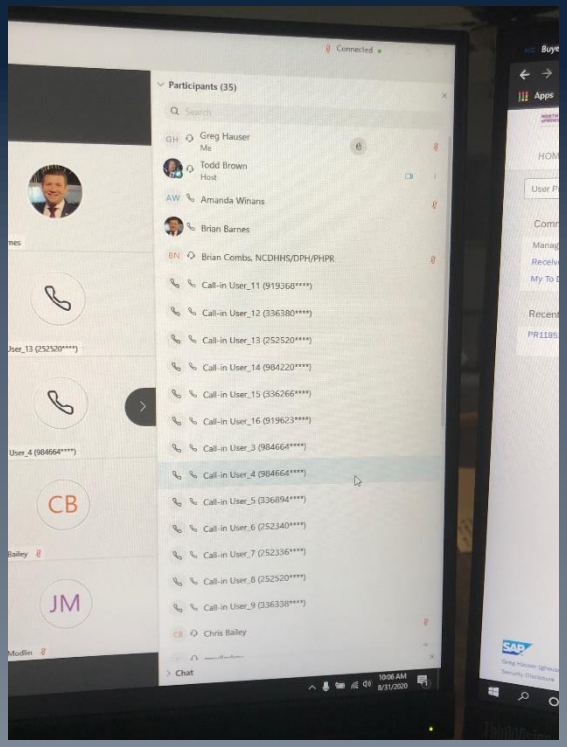


Accurate as of 9/28/2020

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

	TLP: RED	TLP: AMBER	TLP: GREEN	TLP: WHITE
Information sharing boundaries	Not for disclosure Restricted to participants only	Limited disclosure Participant organisations only	Limited disclosure Restricted to community only	Disclosure is not limited
When to use	Impacts privacy, reputation or operations	Risk to privacy, reputation or operations if shared outside participating organisations	Useful for participating organisations and broader community	Minimal or no foreseeable risk of misuse, suitable for public release
How to share	Participating organisations only	Organisation members only. Additional restrictions can be set.	Peer and partner organisations only. Not suitable for public release	No restrictions



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

Help is sent

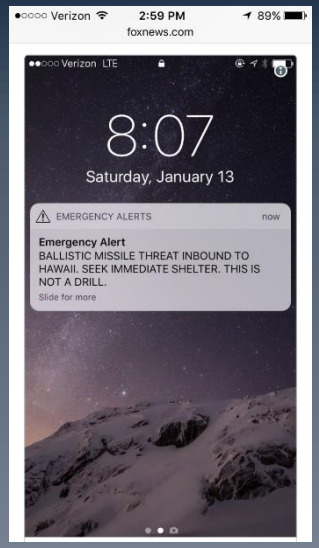
Public Information Availability

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

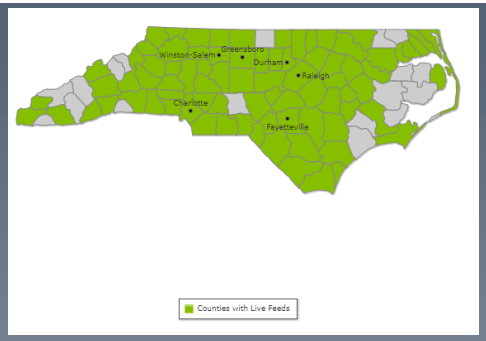
Problem is/isn't resolved

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

Problem is/isn't resolved

- 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.

Actions and options

North Carolina Emergency Management
Communications Branch

Informational Bulletin

TLP: AMBER – Limited Disclosure

Date: May 31, 2020

To: Public Safety Stakeholders

From: NCEM - 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 NCEM Communications Branch 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 radios. Examples are 8TAC91D, VTAC11, UTAC43D, etc. You also may have

UNCLASSIFIED//FOR OFFICIAL USE ONLY

INTELLIGENCE ENTERPRISE

Homeland Security

INTELLIGENCE NOTE

31 May 2020

(U//FOUO) Potential for Illicit Actors Monitoring and Disrupting Law Enforcement Communications During Ongoing Violence

(U//FOUO) **Scope.** This *Intelligence Note* (*IN*) provides information regarding targeted violence threatening homeland security at otherwise lawful protests related to recent officer-involved deaths and highlights the concern that illicit actors, including potentially domestic violent extremists (DVEs)[a], could take advantage of widely available resources to monitor, exploit and compromise law enforcement communications. The information in this *IN* is current as of 31 May 2020.

(U//FOUO) We assess that illicit actors seeking to incite violence at otherwise lawful protests probably are monitoring local law enforcement communications to identify vulnerabilities in their operational security posture. The emergence of publicly accessible applications allows users to search and listen to law enforcement channels streaming online, potentially providing illicit actors insight into operational planning and response efforts. Some technically advanced actors may seek to undermine law enforcement's situational awareness and ability to coordinate operations by disrupting or interfering with law enforcement communications.

» (U//FOUO) As of 30 May, law enforcement officials in Portland, Oregon reported that they assessed that well-coordinated groups had potentially compromised law enforcement radio communications, according to DHS operational information.[1] Police officers in Minneapolis earlier this week were forced to switch to cell phones for tactical communications after learning their communications were being monitored by individuals using publicly available police scanner apps to disrupt law enforcement operations, according to unverified press reporting.[2]

» (U) Unidentified individuals reportedly were able to disrupt law enforcement communications in the Chicago area after police frequencies were publicly posted on the internet, allowing unidentified individuals to saturate the channels with music, according to media reporting.[3]

» (U//FOUO) In June 2018, a self-identified anarchist extremist[a] obtained information related to Federal Protective Service operations and security personnel by monitoring a law enforcement communications, according to DHS reporting. The anarchist extremist later posted the information online using a hashtag associated with protests against DHS immigration enforcement operations.[4] Anarchist extremists in December 2017 discussed implications for disrupting law enforcement communications in a social media thread seeking to incite violent acts of sabotage targeting law enforcement, according to DHS reporting.[5]

Questions?

THANK YOU!