Public Safety Communications Networks

Information Sharing and Expectation Management

2021 N.C. Cybersecurity Symposium

Speakers

- Greg Hauser – North Carolina Emergency Management

  Communications Branch Manager/SWIC

- Carly Sherrod – North Carolina Emergency Management

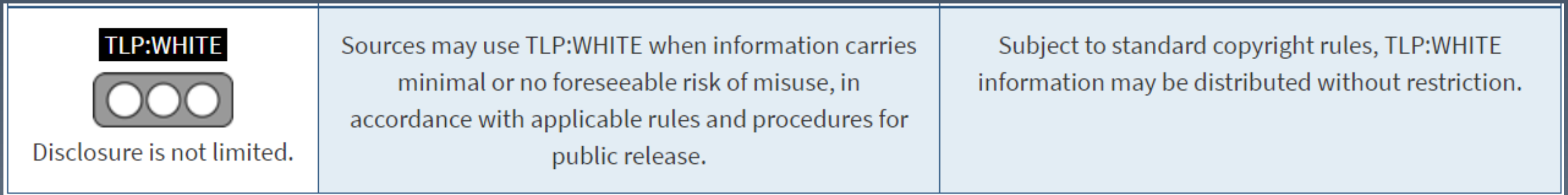
  Homeland Security Branch, NC Joint Cybersecurity Task Force

Contributions to presentation material made by:

- Matt Runyan – Cisco Crisis Response (fka Cisco TacOps)

Goal

- Provide attendees with a broad look at public safety communications information sharing vulnerabilities while focusing on consequence management following an event.



TLP:WHITE ○○○ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

https://www.cisa.gov/tlp

Objectives

- Provide common gaps identified in previous events, trainings and exercises.
- Provide insight into disaster based communications processes.

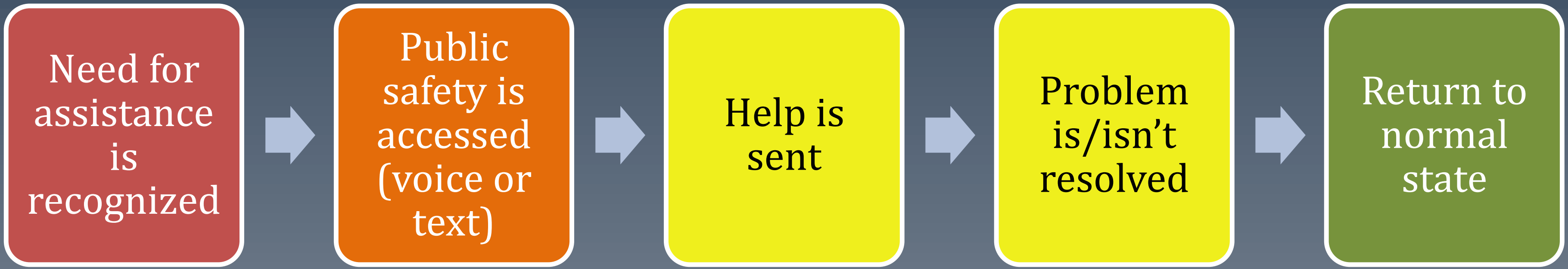
Accurate as of 10/4/2021

Disclaimer

- This presentation is not intended to cast judgement on first response or IT entities. Examples given are intended to show lessons learned, not spotlight gaps.

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.



Need for assistance is recognized

Public safety is accessed (voice or text)

Help is sent

Problem is/isn’t resolved

Return to normal state

Common Communications Gaps Between First Responders and IT

First Responders

Fix issues as quick as possible; move on to the next issue. Lifesaving Environmental/Property conservation. "Short-Term Fixes" in IT-speak

IT Professionals

Focus on Short-Term and Long-Term Fixes. Incorporate a change management process. Approach an issue in a methodical manner. A missed step could add to down time.

Similar Approaches Between First Responders and IT

First Responders

Fix a problem following agency guidelines when possible, improvising when needed.

IT Professionals

Follow a process in accordance with an approved procedure/policy, improvising when needed.

Common Consequences to communications gaps

First Responders

“I’m gonna try and fix this myself. (clicks various links and files)

IT Professionals

“I don’t have time for these people, we’ll fix it when we can” (tunes out first responder feedback)

Common Consequences to communications gaps

First Responders

“All they do is complain”

IT Professionals

“All they do is complain”

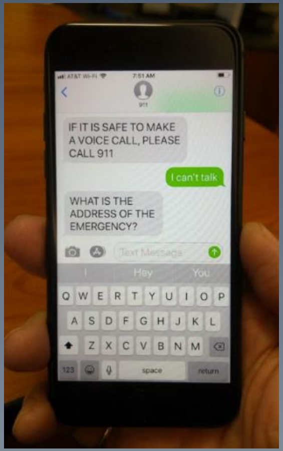
Recommendations

1. Agree on the solution, not the problem.
2. Communicate the expectations and find a common adversary.
3. Establish lanes of communications, i.e. where does information get exchanged?
4. ICS works, give it a try.
5. Being methodical works, give it a try.

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?
- What reliance do your agencies have on cellular voice and data networks?
  - Internal governmental notifications
  - No notice events (Nashville, TN)



IF IT IS SAFE TO MAKE A VOICE CALL, PLEASE CALL 911

I can't talk

WHAT IS THE ADDRESS OF THE EMERGENCY?

Accurate as of 10/4/2021

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 operate in a degraded environment?
  - Processes?
  - Staffing?
  - Realistic expectations – Be honest

Consequence Management Process

Communicate

- Local Public Safety/Emergency Management/911
- Local Public Health
- Local Board of Elections
- Local Board of Education
- Others?

Consequence Management Process

Public Safety Concerns

- Ensuring the safety of the public.
- Ensuring open lines of communication with staff.
- What do we tell people with out inciting fear and the sense of the unknown.

Consequence Management Process

Cyber Incident Response Process

- Preparation
- Identification (Detection and Analysis)
- Containment
- Eradication
- Recovery
- Lessons Learned/Post-Incident Activity

North Carolina Joint Cybersecurity Task Force

Training being conducted for our SLTT partners

- NCNG/NCEM/NCDIT/NCLGISA provide In-Person and Virtual trainings

During a Blue-Sky Day, a cyber attack is the victim's hurricane

- Services are down
- EM needs to assist in traditional ways as well

Local/Area Public Safety personnel are building relationships with IT departments (CIOs etc.) before event

- Assist with preparation
- Assist with Incident Management
- This is new (and potentially scary and uncomfortable) for the victim

Cybersecurity Assessment Tools Available

Accurate as of 10/4/2021

Questions?

THANK YOU!

Carly Sherrod – NCEM, Joint Cybersecurity Task Force

Carly.Sherrod@ncdps.gov

Greg Hauser – NCEM Communications Branch

Greg.hauser@ncdps.gov

Contributor – Matt Runyan – Cisco Crisis Response (fka TacOps)

matrunya@cisco.com