EMERGENCY MANAGEMENT N★C NORTH CAROLINA

North Carolina
Emergency Management

EMERGENCY MANAGEMENT EMAP Accredited ACCREDITATION PROGRAM

N★C DPS DEPARTMENT OF PUBLIC SAFETY

Information Technology During Disasters

Does IT and Cybersecurity Matter?

NORTH CAROLINA STATE INTEROPERABILITY EXECUTIVE COMMITTEE

2022 N.C. Cybersecurity Symposium

Speakers

- Greg Hauser – North Carolina Emergency Management

  Communications Branch Manager/SWIC

- Jeff Martin – Town of Mooresville

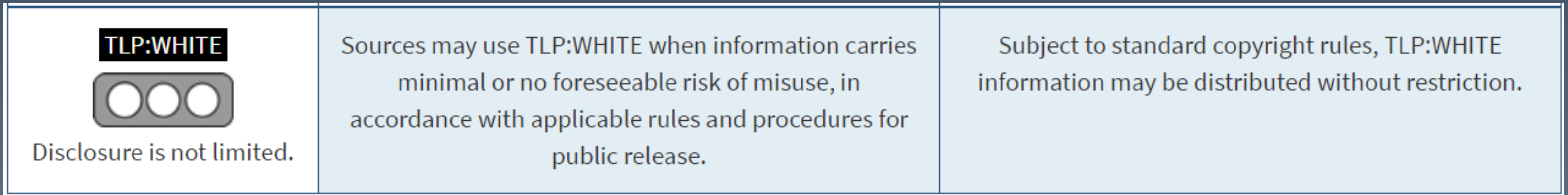
  Deputy Technology & Innovation Director

Contributions to presentation material made by:

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

Goal

- Provide attendees with an understanding of how Information Technology (IT) integrates into disaster response and the Incident Command System (ICS)



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 guidance for stakeholders to integrate IT services and expertise into planning, response and recovery.
- Provide a basic understanding of ICS practices during disasters.

Information Technology During Disasters

WAS

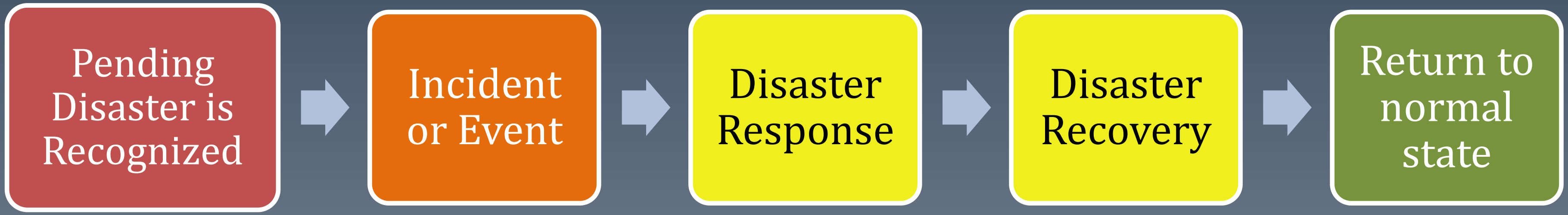
Information Technology During Disasters

IS

- An immediate need for all layers of disaster response.
- The most vital puzzle piece for open information sharing.
- The most taken for granted.
- The most vulnerable.

Incident Management Cycle

- Process of managing incident actions.
- Provides process to each phase of a response.



IT based pre-planning processes: The basics

- Identify and test equipment / systems.
- Understand dependencies and weak points.
- Verify fuel and battery charge levels of generators, UPS equipment.
- Charge batteries, update firmware and patch software of cache equipment.

IT based pre-planning processes: Cybersecurity-specific

- Educate users about ticket reporting processes.
- Reinforce cybersecurity priorities and cyber hygiene.
- Keep your guard up (re: links and attachments): You’re tired and stressed. One click on a bad link can throw a monkey wrench into entire response.

IT based response actions

- Communications and IT Support are early requests by Incident Commanders
- The ability to communicate upstream and downstream is critical to achieving incident objectives.
- Conditions can often be austere requiring flexible responses to technical problems.
- Cyber risks must still be considered no matter the location or situation.

IT based response actions continued

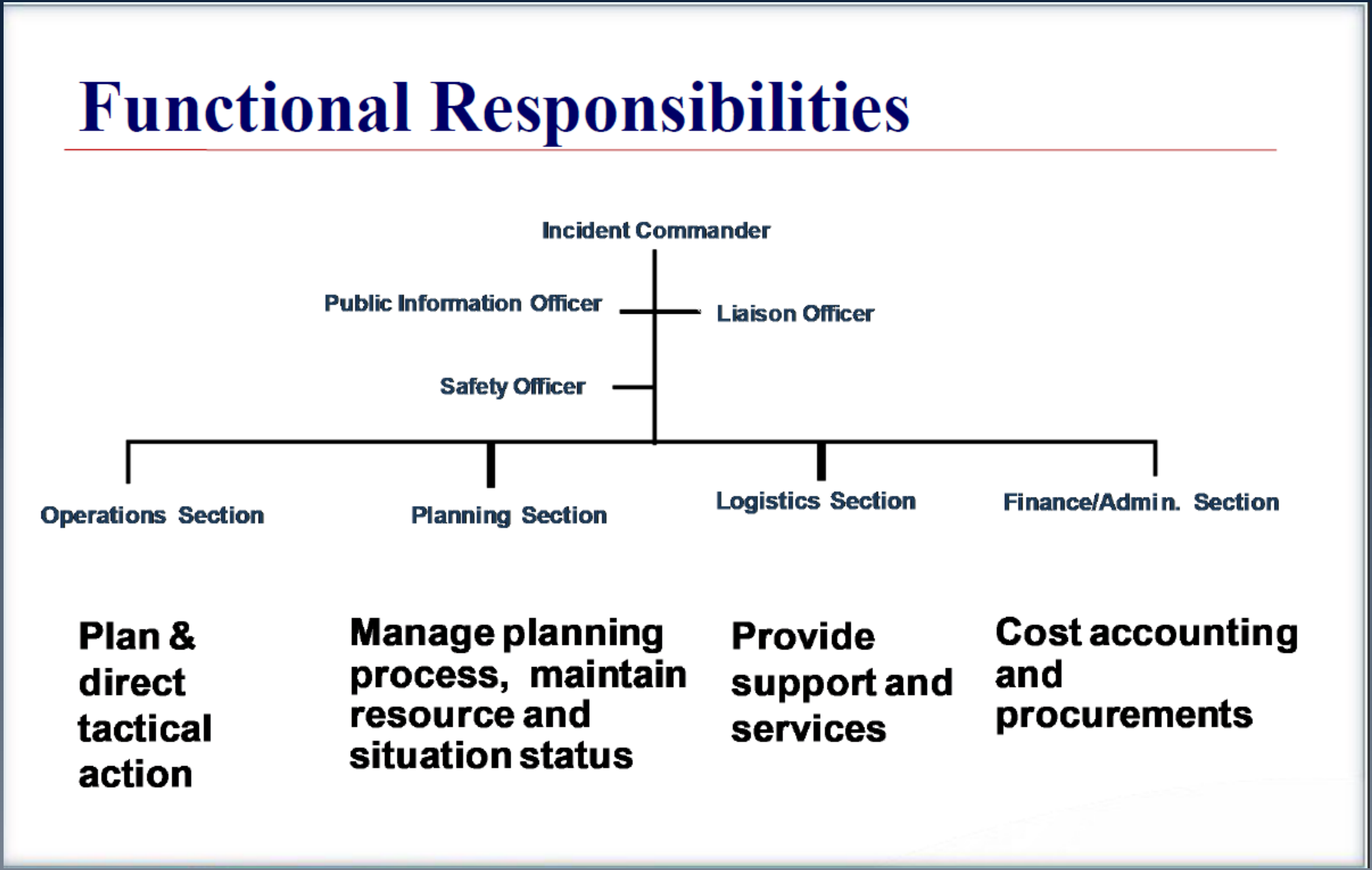
- Conduct PACE Planning for mission-critical systems / capabilities
- Monitor critical systems / assets
- Back up your data in 3 places:
  local primary, local backup, offsite backup.
- Consider temporary systems vs. day-to-day.
  (integrated or air-gapped?)
- Grant minimum access people need to do their jobs.
- Record changes made to be reverted after incident, especially firewalls, access granted to individuals.

Incident Command System (ICS)

- A standard way of managing and incident from the local or scene level.
- Flexible and scalable.
- Provides a means to support all operational aspects of on scene activity.

https://training.fema.gov/is/

Incident Command System (ICS)



Functional Responsibilities

Incident Commander

Public Information Officer

Liaison Officer

Safety Officer

Operations Section

Planning Section

Logistics Section

Finance/Admin. Section

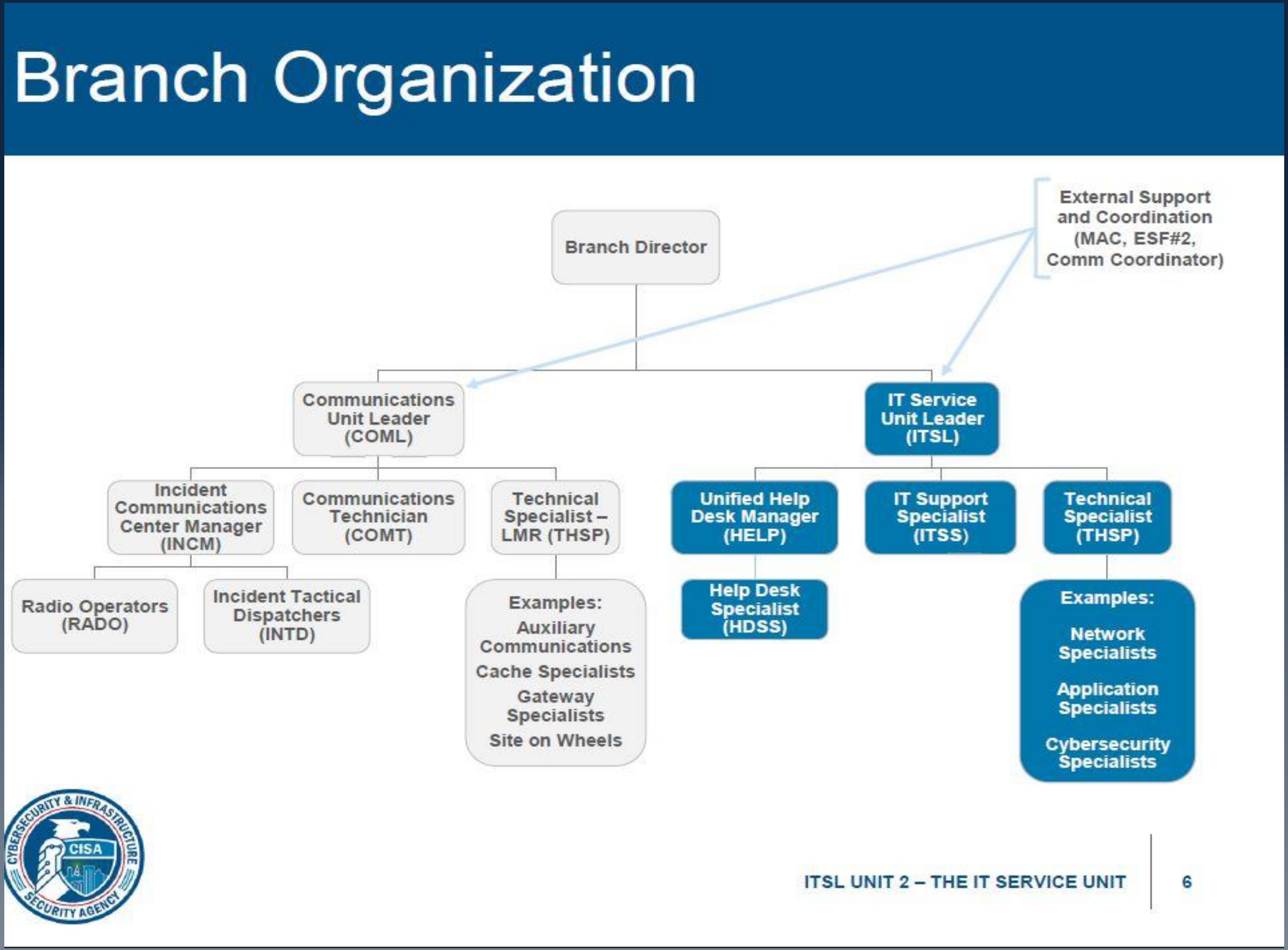
Plan & direct tactical action

Manage planning process, maintain resource and situation status

Provide support and services

Cost accounting and procurements

ICS Branch Structure



Branch Organization

Branch Director

External Support and Coordination (MAC, ESF#2, Comm Coordinator)

Communications Unit Leader (COML)

- Incident Communications Center Manager (INCM)
  - Radio Operators (RADO)
  - Incident Tactical Dispatchers (INTD)
- Communications Technician (COMT)
- Technical Specialist – LMR (THSP)
  - Examples: Auxiliary Communications; Cache Specialists; Gateway Specialists; Site on Wheels

IT Service Unit Leader (ITSL)

- Unified Help Desk Manager (HELP)
  - Help Desk Specialist (HDSS)
- IT Support Specialist (ITSS)
- Technical Specialist (THSP)
  - Examples: Network Specialists; Application Specialists; Cybersecurity Specialists

ITSL UNIT 2 – THE IT SERVICE UNIT | 6

Finding the right balance

- Incident based support
  - Wants vs. Needs
  - Current capabilities vs. Added capabilities
- Finding the right capability to fill an identified gap.
- Achieving IT and cyber goals while supporting the incident.

IT based recovery actions

- Consider transition back to “normal operations”. When/how to demobilize IT assets/staff?
- Plan for disposition of data created during incident: who keeps what? where? how long?
- Disable firewall rules / accounts / access no longer needed.

Questions?

THANK YOU!

Jeff Martin – Town of Mooresville

Jmartin@mooresvillenc.gov

Greg Hauser – NCEM Communications Branch

Greg.hauser@ncdps.gov

Contributor – Matt Runyan – Cisco Crisis Response

matrunya@cisco.com