EMERGENCY MANAGEMENT & CYBERSECURITY

BRIDGING THE GAP

AGENDA

- What are we trying to solve?
- Identify obstacles
- Steps to take
- Exercises
- Continuing relationships

WHAT ARE WE TRYING TO SOLVE?

CYBER INCIDENT RESPONSE IS ALL OVER THE BOARD. THE PROCESS DIFFERS WILDLY FROM ORGANIZATION TO ORGANIZATION.

EMERGENCY MANAGEMENT HAS A DEFINED STRUCTURE BUT HAS NOT INCORPORATED CYBER INTO THE MIX.

IDENTIFY OBSTACLES

JARGON BARRIERS

BUY-IN <TOP AND **BOTTOM**>

DIFFERENT STRUCTURES

MUTUAL INTELLIGENCE ACKNOWLEDGEMENT

STEPS TO TAKE….

STEP 1….

- Start with a conversation with the Office of Emergency Management
  - Get rid of ***ALL*** acronyms during this conversation
  - How does the Incident Command Structure work?
  - What materials are used to communicate?
  - What does escalation look like?
  - Who fills the Incident Command Structure roles?
  - How are they chosen?
  - How are they trained?

STEP 2….

- Find common ground
  - What emergency best fits your organization as a metaphor?
  - What things have you already built that can support the Incident Command structure?
  - What relationships already exsist between Information Technology and Office of Emergency Management?

STEP 3….

- Start a conversation…… with Information Technology!
  - Same rule applies…. Get rid of ***<u>ALL</u>*** acronyms during this conversation
  - Understand current Incident Response in your organization
  - Compare – what is the same?
  - What are our hanging points? (Put in a pin in this)

STEP 4….

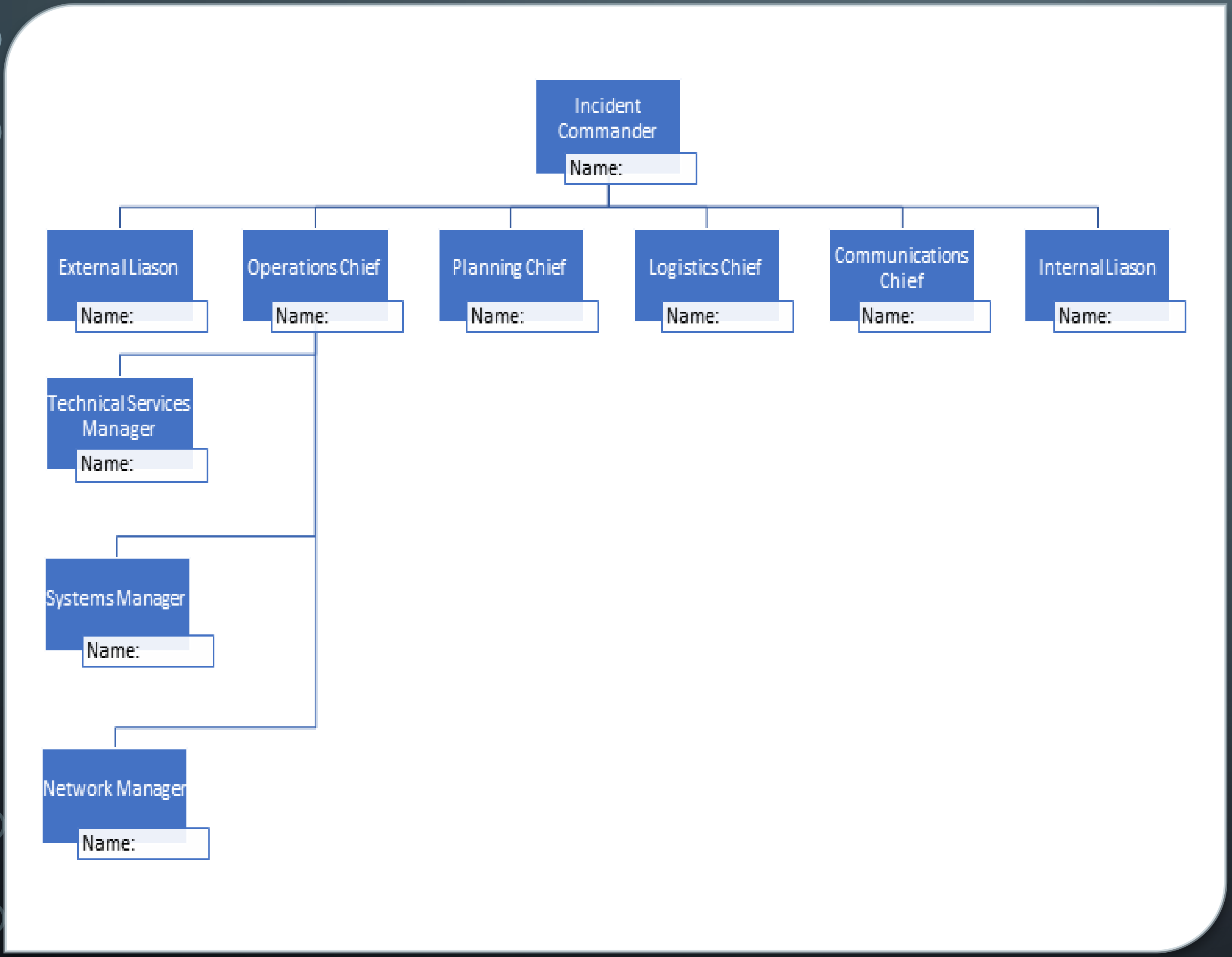
- Schedule a training for Information Technology staff on the Incident Command Structure
- Ask the Emergency Management staff if we can cater to information technology in this training.
    - If not…Call up Arapahoe County Office of Emergency Management, and ask about IT oriented NIMS Training

STEP 5….

- Build internal Incident Command Structure
  - Assign Incident Command Structure roles
    - Multiple people for each role
  - Identify what Command Structure looks like
  - Checklists for each role
  - General Playbook for Incident
  - Create and organize what briefs look like
  - Develop a contact repository
  - Activity Log
  - Keep it all in one place

SAMPLE STRUCTURE

- Include roles necessary,
  - i.e. managers of operational teams



Incident Commander
Name:

External Liason
Name:

Operations Chief
Name:

Planning Chief
Name:

Logistics Chief
Name:

Communications Chief
Name:

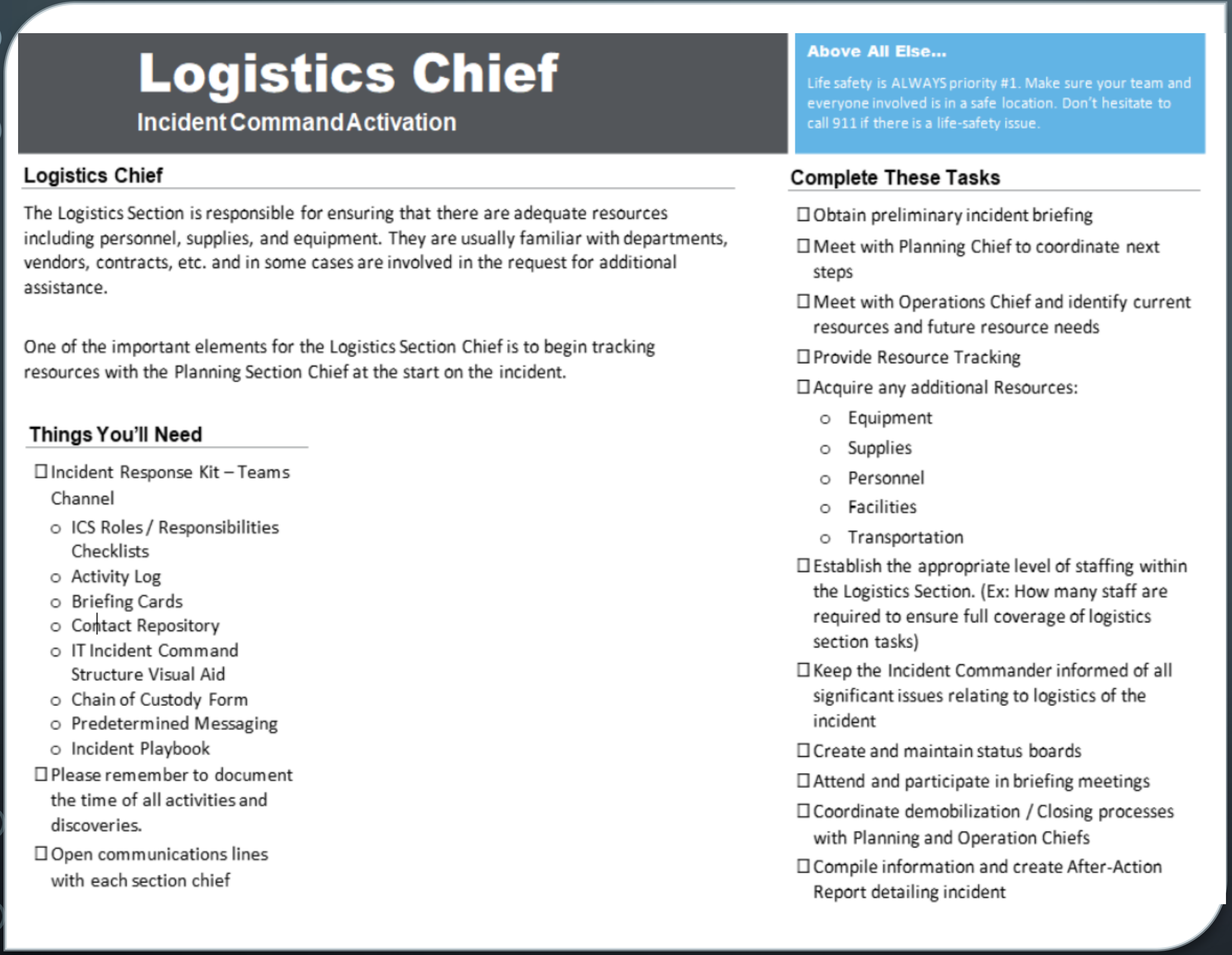
Internal Liason
Name:

Technical Services Manager
Name:

Systems Manager
Name:

Network Manager
Name:

SAMPLE ROLE REFERENCE CARD



Logistics Chief

Incident Command Activation

Above All Else...

Life safety is ALWAYS priority #1. Make sure your team and everyone involved is in a safe location. Don't hesitate to call 911 if there is a life-safety issue.

Logistics Chief

The Logistics Section is responsible for ensuring that there are adequate resources including personnel, supplies, and equipment. They are usually familiar with departments, vendors, contracts, etc. and in some cases are involved in the request for additional assistance.

One of the important elements for the Logistics Section Chief is to begin tracking resources with the Planning Section Chief at the start on the incident.

Things You'll Need

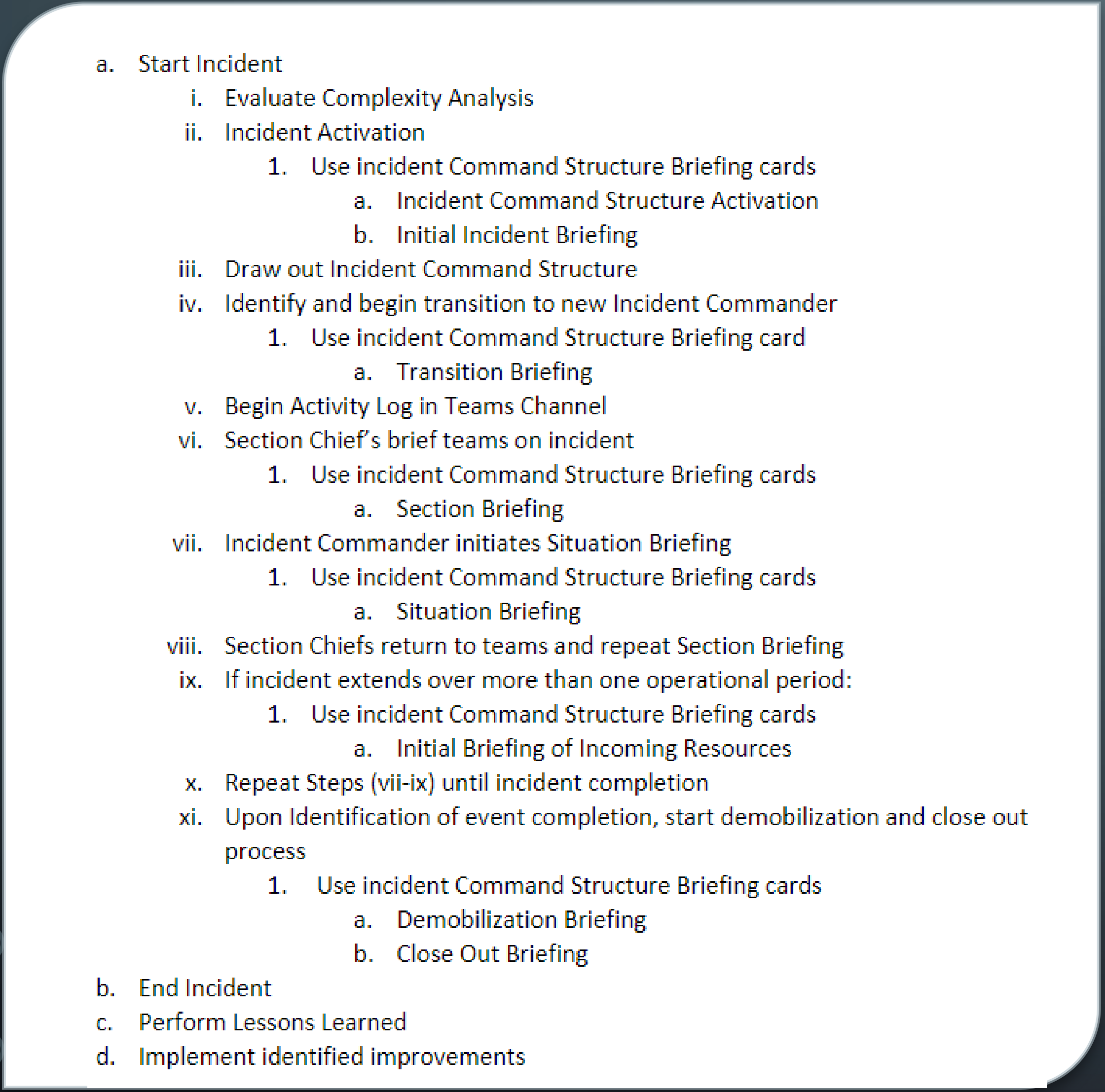
- □ Incident Response Kit – Teams Channel
  - ICS Roles / Responsibilities Checklists
  - Activity Log
  - Briefing Cards
  - Contact Repository
  - IT Incident Command Structure Visual Aid
  - Chain of Custody Form
  - Predetermined Messaging
  - Incident Playbook
- □ Please remember to document the time of all activities and discoveries.
- □ Open communications lines with each section chief

Complete These Tasks

- □ Obtain preliminary incident briefing
- □ Meet with Planning Chief to coordinate next steps
- □ Meet with Operations Chief and identify current resources and future resource needs
- □ Provide Resource Tracking
- □ Acquire any additional Resources:
  - Equipment
  - Supplies
  - Personnel
  - Facilities
  - Transportation
- □ Establish the appropriate level of staffing within the Logistics Section. (Ex: How many staff are required to ensure full coverage of logistics section tasks)
- □ Keep the Incident Commander informed of all significant issues relating to logistics of the incident
- □ Create and maintain status boards
- □ Attend and participate in briefing meetings
- □ Coordinate demobilization / Closing processes with Planning and Operation Chiefs
- □ Compile information and create After-Action Report detailing incident

- Brief Description
- What tasks are the responsibility of this role?
- What does this role need to be successful?
- Any additional information (Direct reports, Procedure locations, etc)

GENERAL PLAYBOOK OUTLINE



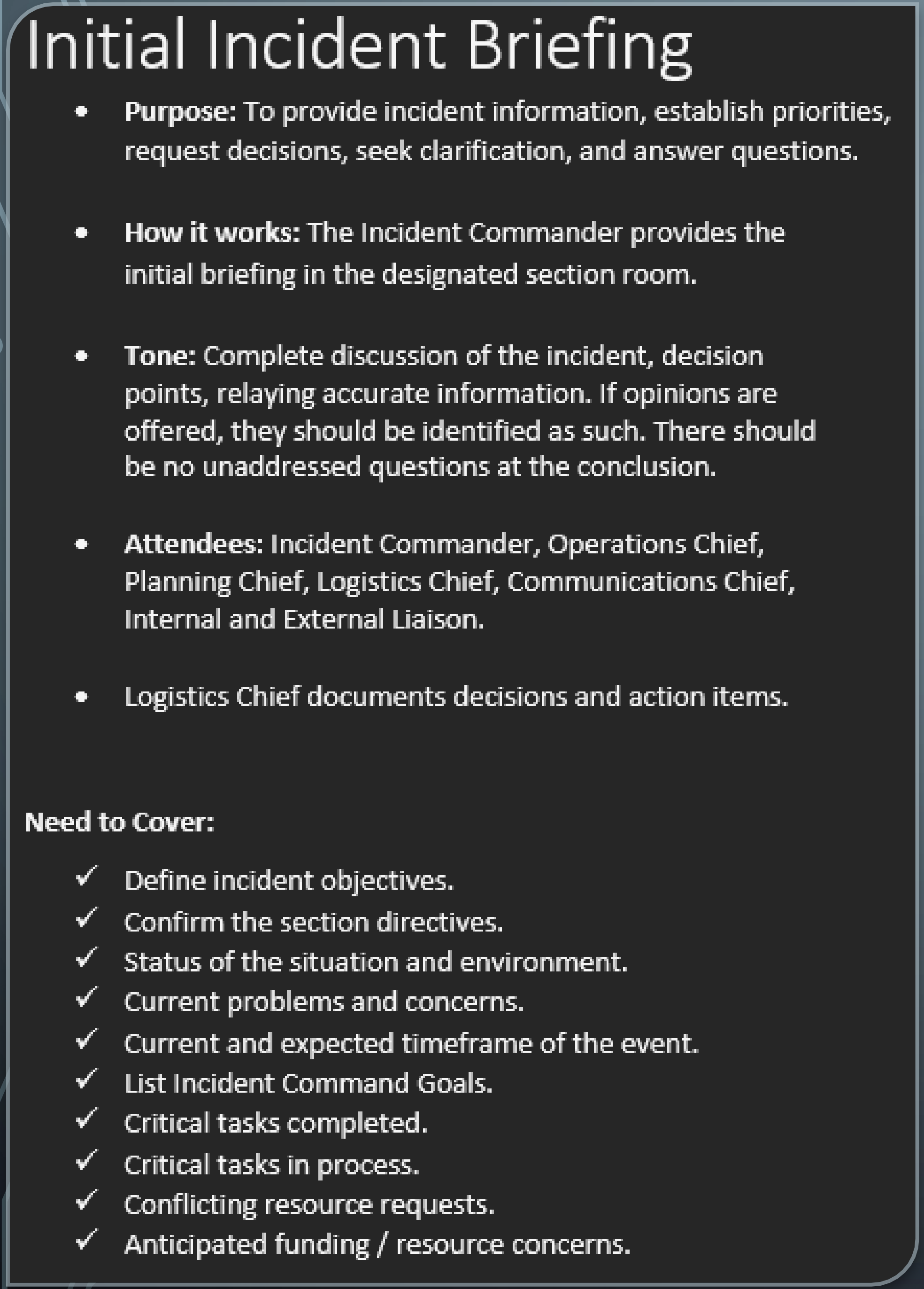
- a. Start Incident
  - i. Evaluate Complexity Analysis
  - ii. Incident Activation
    - 1. Use incident Command Structure Briefing cards
      - a. Incident Command Structure Activation
      - b. Initial Incident Briefing
  - iii. Draw out Incident Command Structure
  - iv. Identify and begin transition to new Incident Commander
    - 1. Use incident Command Structure Briefing card
      - a. Transition Briefing
  - v. Begin Activity Log in Teams Channel
  - vi. Section Chief's brief teams on incident
    - 1. Use incident Command Structure Briefing cards
      - a. Section Briefing
  - vii. Incident Commander initiates Situation Briefing
    - 1. Use incident Command Structure Briefing cards
      - a. Situation Briefing
  - viii. Section Chiefs return to teams and repeat Section Briefing
  - ix. If incident extends over more than one operational period:
    - 1. Use incident Command Structure Briefing cards
      - a. Initial Briefing of Incoming Resources
  - x. Repeat Steps (vii-ix) until incident completion
  - xi. Upon Identification of event completion, start demobilization and close out process
    - 1. Use incident Command Structure Briefing cards
      - a. Demobilization Briefing
      - b. Close Out Briefing
- b. End Incident
- c. Perform Lessons Learned
- d. Implement identified improvements

- Keep it short
- Be concise
- Leave it high level

BRIEFING CARDS

- Purpose of meeting
- How it works
- Tone of Meeting
- Attendees
- Need to cover items

SAMPLE BRIEFING CARD



Initial Incident Briefing

- **Purpose:** To provide incident information, establish priorities, request decisions, seek clarification, and answer questions.

- **How it works:** The Incident Commander provides the initial briefing in the designated section room.

- **Tone:** Complete discussion of the incident, decision points, relaying accurate information. If opinions are offered, they should be identified as such. There should be no unaddressed questions at the conclusion.

- **Attendees:** Incident Commander, Operations Chief, Planning Chief, Logistics Chief, Communications Chief, Internal and External Liaison.

- Logistics Chief documents decisions and action items.

Need to Cover:

- ✓ Define incident objectives.
- ✓ Confirm the section directives.
- ✓ Status of the situation and environment.
- ✓ Current problems and concerns.
- ✓ Current and expected timeframe of the event.
- ✓ List Incident Command Goals.
- ✓ Critical tasks completed.
- ✓ Critical tasks in process.
- ✓ Conflicting resource requests.
- ✓ Anticipated funding / resource concerns.

TYPES OF BRIEFING CARDS TO CREATE…

- Incident Command Structure Activation
- Initial Incident Briefing
- Section Briefing
- Initial Briefing of Incoming Resources
- Situation Briefing
- Transition Briefing
- Close Out Briefing
- Demobilization Briefing

OTHER CONSIDERATIONS…

1

Include real time activity log that EVERYONE in incident has access to.

2

Be mindful of Decision Fatigue and document anything you can ahead of time

- Predetermined messaging
- Playbooks of each team's operations with procedures
- Etc

3

Keep it all in one place and ready to go!!!!!

STEP 6…

- Exercise what you have learned
- Include each role
- Practice the briefing cards
- Practice quick concise communication
- Practice what documenting looks like
- Practice. Practice. Practice.

STEP 7…

- Maintain relationships and build trust!!
- Regular Meetings (quarterly or more)
- Spend time reviewing plans
- BE TRANSPARENT!

?

QUESTIONS