

<https://github.com/Hnikar-az/bshq>



Cyber Incident Command System

A People Orchestration Layer

Blake, Scott





Disclaimer

This presentation not represent the positions, policies, or procedures of the United States Government, the places we work, or volunteer for.



Agenda

- The Problem (A State Of Confusion)
- Introduce the solution
- Example of the solution at work - A quick hospital story
- The Systems
- Would you like to know more?



The Problem

- We're stuck with the people we have during an incident.
 - Meaningful resource sharing does not exist.
- Existing systems are dangerous to responders

Photo by [Anders Norrback Bornholm](#) on
Unsplash



A glowing neon sign is mounted on a dark brick wall. The sign features the words "THERE IS A BETTER WAY" in a bold, sans-serif font. The letters are white against a red background, and the sign is illuminated from behind, casting a warm glow on the surrounding wall. Above the sign, a metal pipe runs horizontally across the wall, with a vertical section extending downwards. The overall atmosphere is gritty and urban.

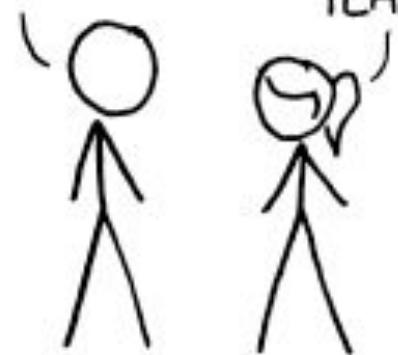
THERE IS A BETTER WAY

HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



YEAH!

SOON:

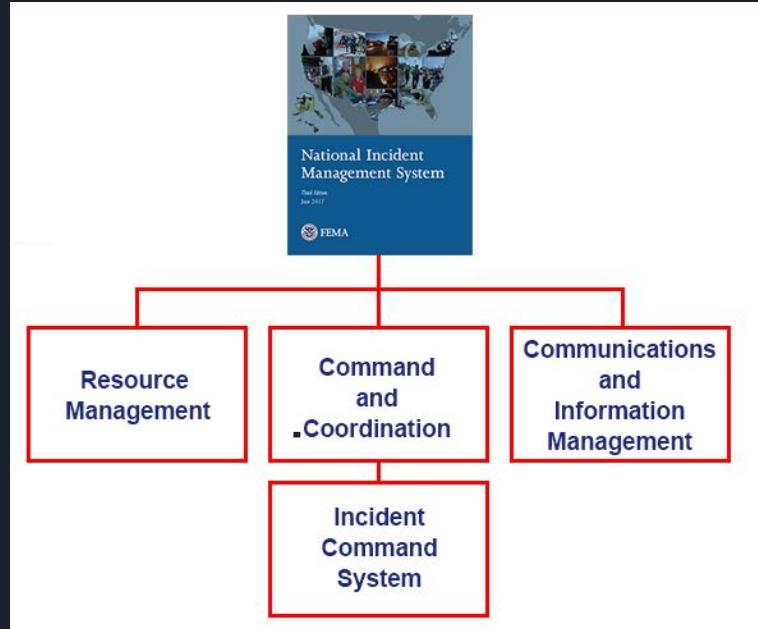
SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

National Incident Management System

- A people orchestration layer

Results in & Contains Information About:

- Staff Safety
- Transferable Operations



<https://training.fema.gov/is/coursematerials.aspx?code=IS-100.c> IS-100.C: Introduction to the Incident Command System, ICS 100



Where are we in the system

Manageable Span of Control

Modular Organization

Chain of Command and Unity of Command

Common Terminology

Management by Objective

Comprehensive Resource Management

Establishment and Transfer of Command

Dispatch/Deployment

Incident Action Planning

Incident Facilities and Locations

Integrated Communications

Unified Command

Accountability

Information and Intelligence Management

Cyber Incident Command System - CICS

A People Orchestration Layer

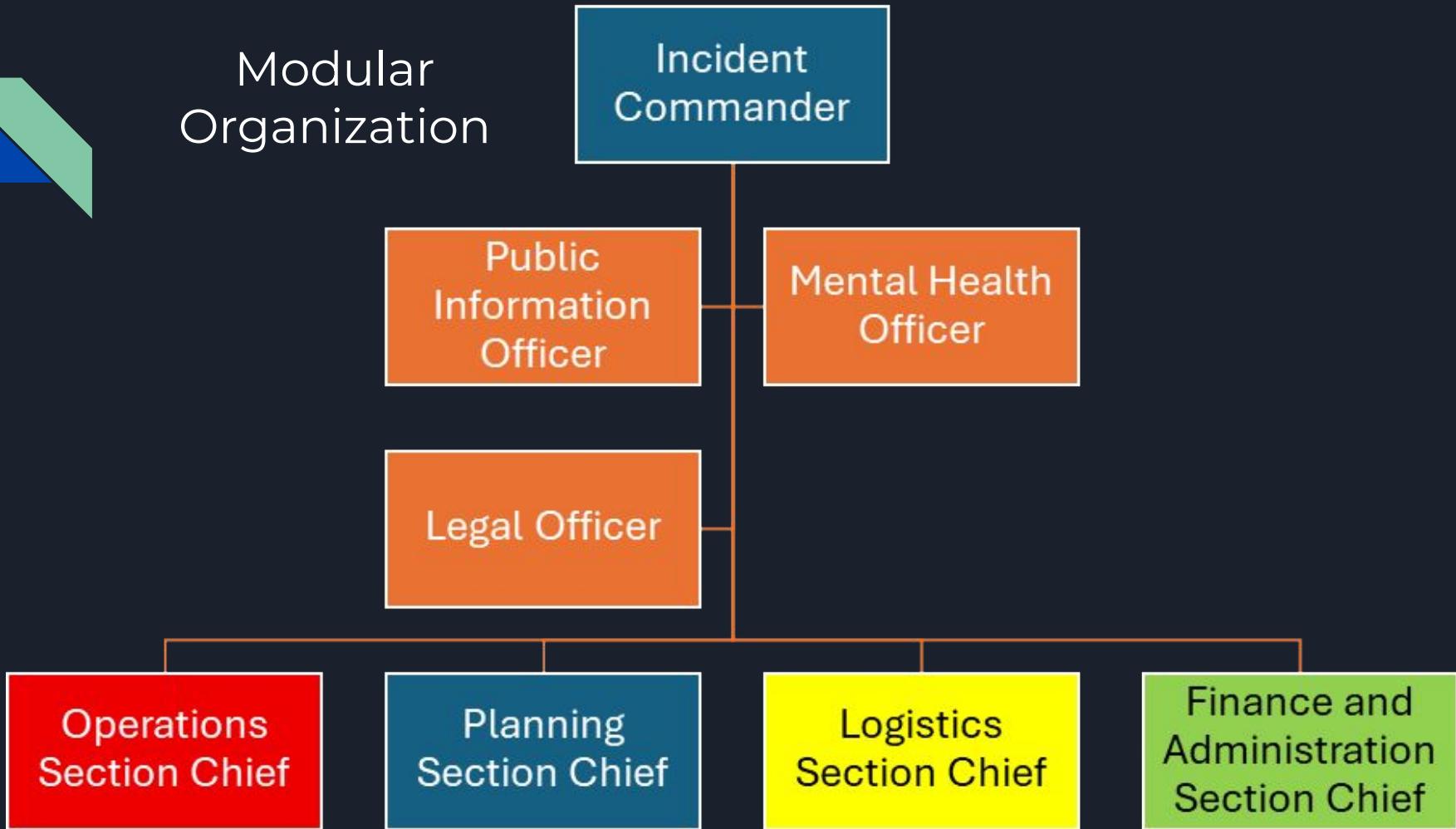
- A lighter version of the National Incident Management System
- Simplified Command and Control Structure

New Role:

- Mental Health Officer Replaces or Augments Safety officer



Modular Organization





Manageable Span of Control



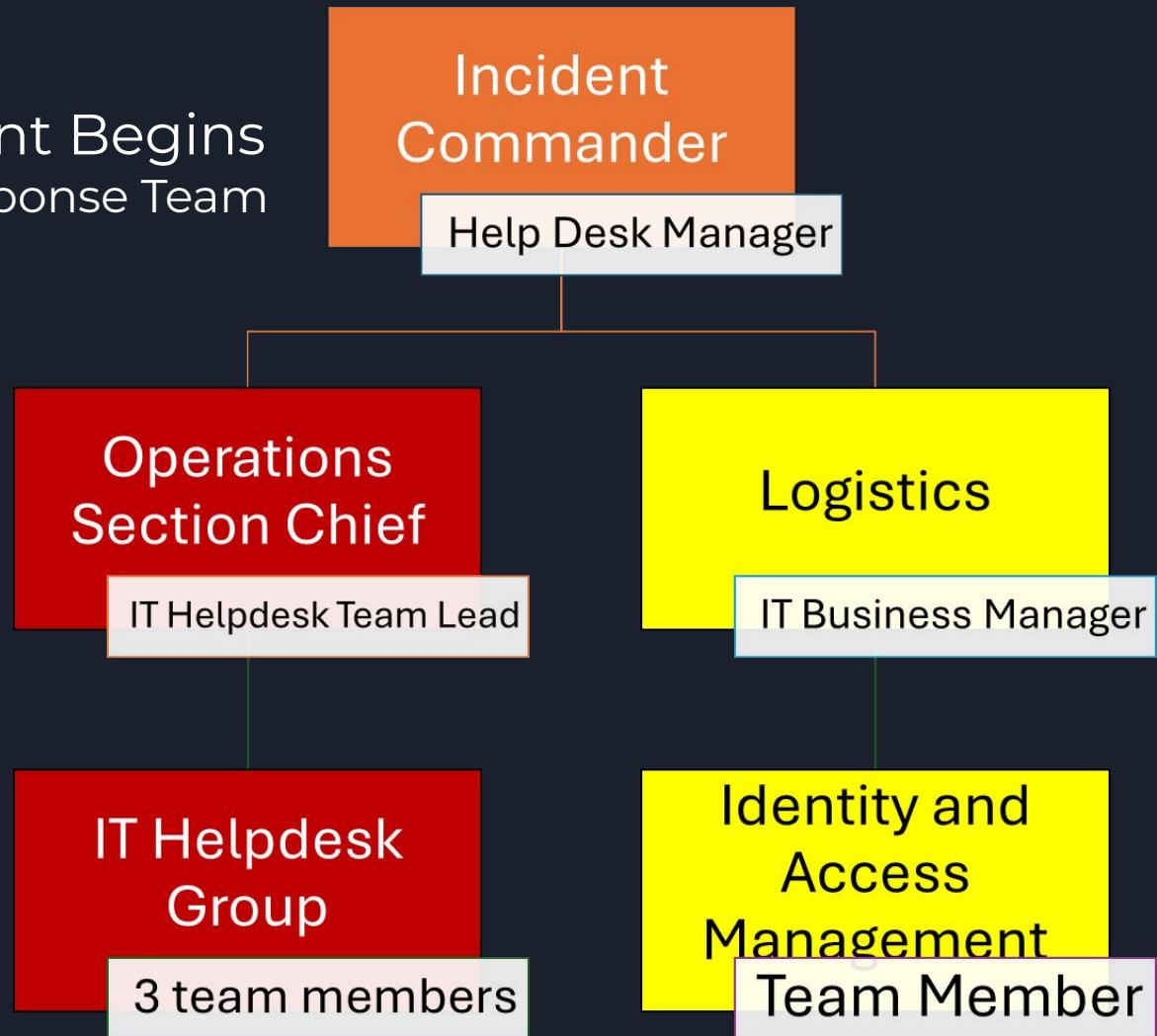
- Best

Story Time - A
problem occurs
So you see what had
happened was

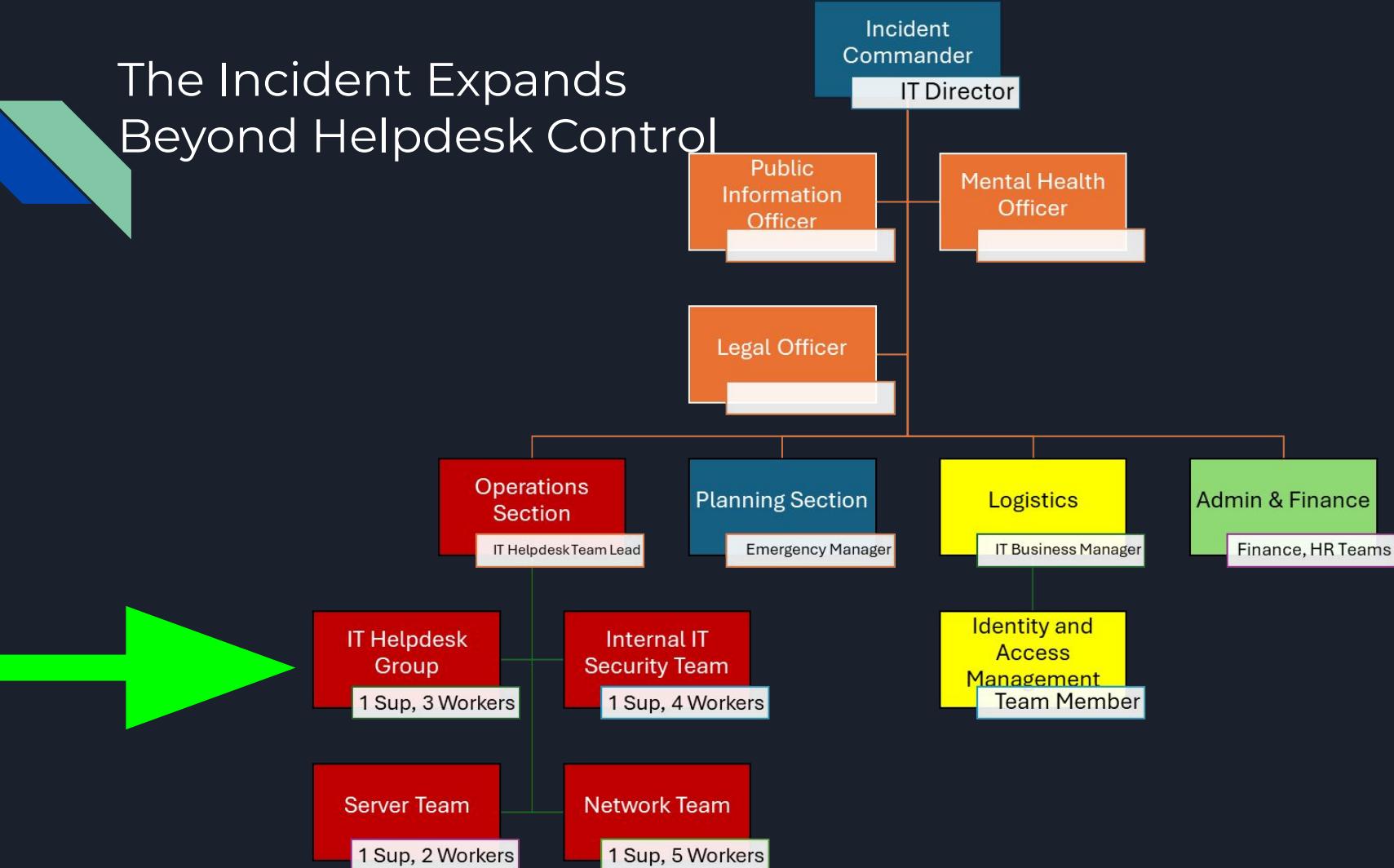




The Incident Begins A Type 5 Response Team

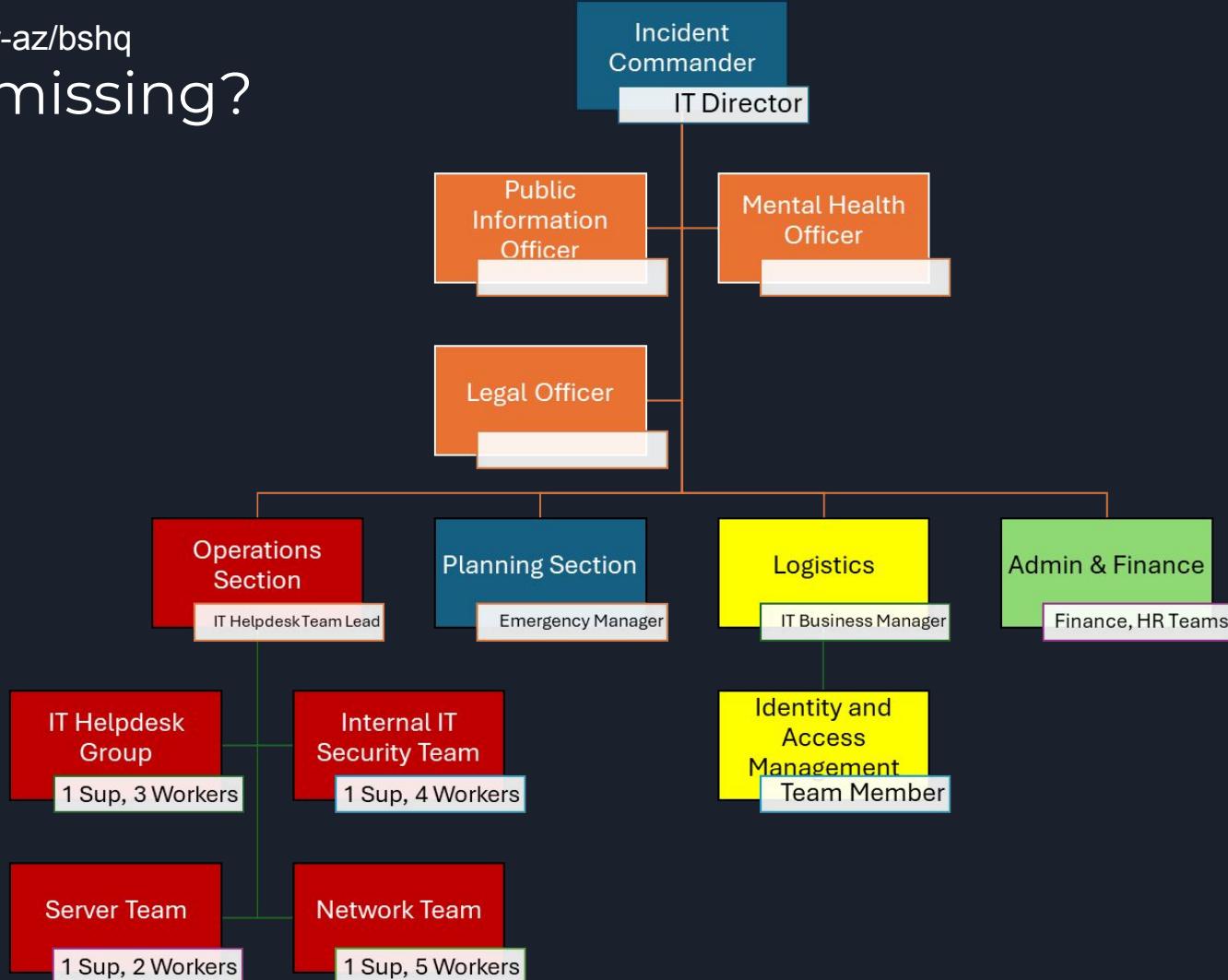


The Incident Expands Beyond Helpdesk Control



Who is missing from that organizational chart?

Who's missing?

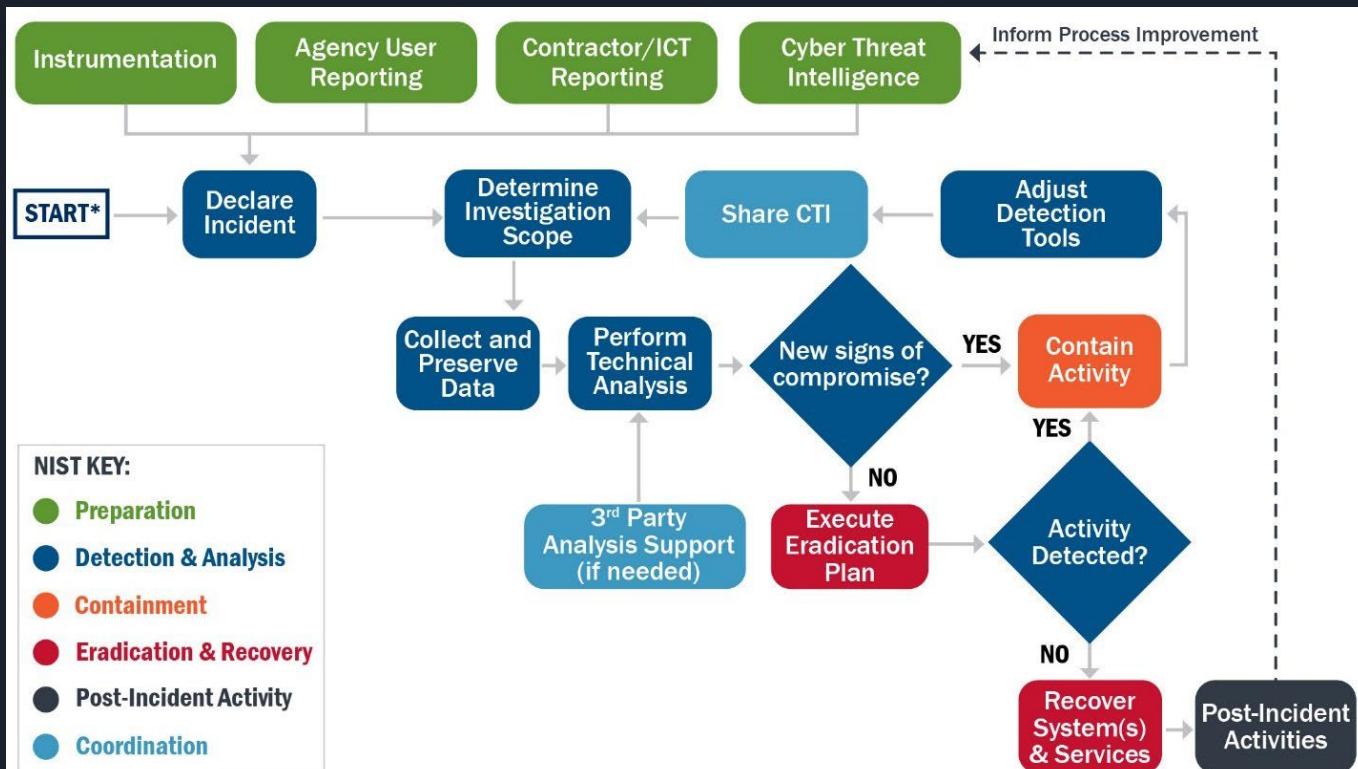


<https://github.com/Hnikar-az/bshq>

The Incident Expands Again



CISA Incident & Vulnerability Response Playbook

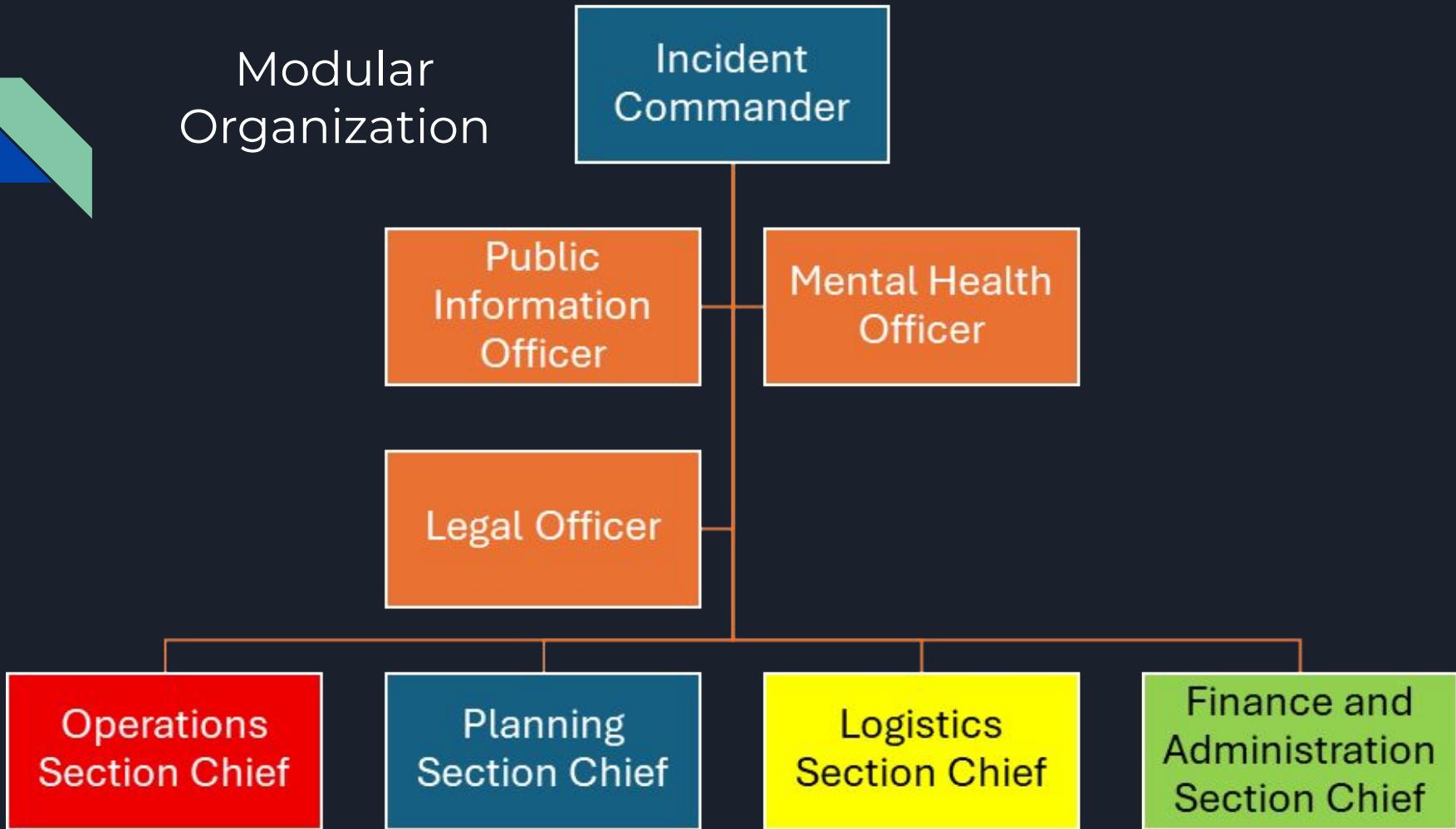


https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

But My Incident Command System Is The Bestestest



Modular Organization

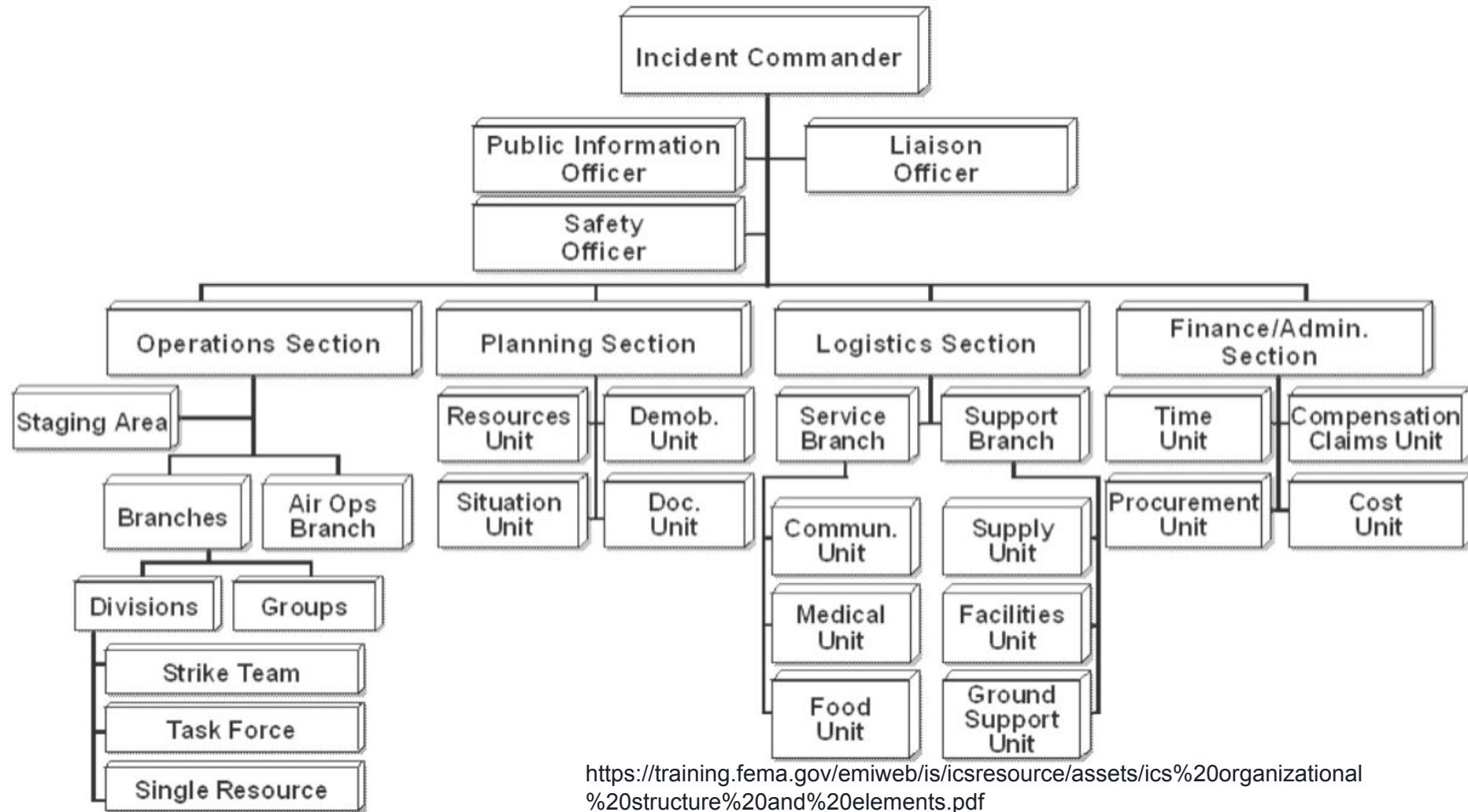




Manageable Span of Control



- Best



Preparedness Summit 2025 - National Association of City and County Health Officials (NACCHO)





The Highlights of Cyber Incident Command System

- Simplified language for faster adoption of the National Incident Management System
- Mental Health officer
- Legal Officer
- Span of Control guidance

The Problem

- We're stuck with the people we have during an incident.
 - Meaningful resource sharing does not exist.
- Existing systems are dangerous to responders



WOULD YOU LIKE TO KNOW MORE?

- FEMA Independent Study Courses
 - *ICS 100 - Introduction to Incident Command System*
 - *ICS 700 - National Incident Management System (NIMS), An Introduction*



Help Build CICS

We need your experience

We want your expertise

Be the Calvary



JOIN UP NOW

- <https://github.com/Hnikar-az/bshq>
- Blake Scott: blake@hnikar.com
- Scott Fraser: scott@codelinenetworks.com

Thank you to the unsplash community for providing us free copyleft images made by human hands. XKCD provided a comic, US government provided some images.

No AI was harmed in the creation of this presentation, all photos in this presentation were made by humans.