Incident Response in Unfamiliar Sociotechnical Systems

One Incident Commander's Challenges Supporting Interorganizational Anomaly Response in the Age of Covid-19

Morgan Collins, Salesforce
mcollins@salesforce.com

What We’re Aiming For In This Talk

An overview of the Incident Command System (ICS)

How ICS has been tuned for private companies

#PandemICS

Touch on learning from your incidents

Why ICS Was Created

The 1960s saw conditions set for increase in wildfire activity in California

The 1970 wildfire season was a doozy

Challenges coordinating all responders and their support organizations

Why ICS Was Created

A task force named FIRESCOPE (Firefighting Resources of California Organized for Potential Emergencies) was established to build what would become ICS

The Objectives:

- Better communications
- Better resource management

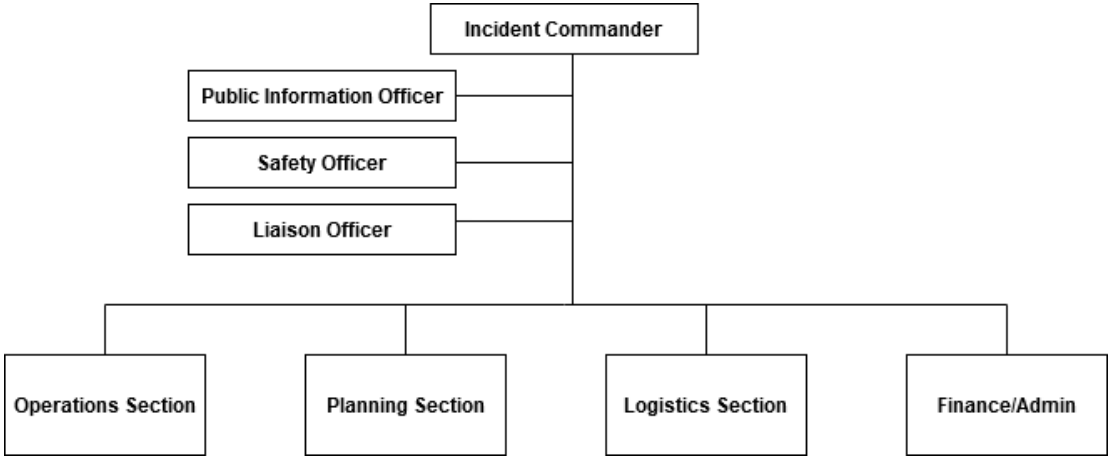
The solution needed to be

- Flexible
- Repeatable
- Cheap

Why ICS Was Created

The Solution

- A centralized leader
- Support staff and support organizations
- Delegation driven
- Report chains



How ICS Has Evolved - NIMS

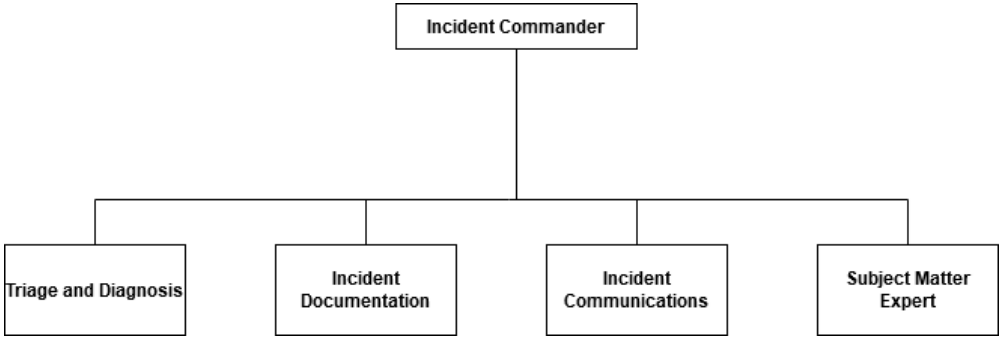
- ICS has continually evolved
- Expansion into how the US conducts international emergency response and military emergency response
- The most recent major iteration of ICS-based incident response has been the National Incident Management System (NIMS)

Successes of ICS Within Private Enterprise

- Repeatable Framework
- Common ground
- Increased system criticality
- Pre-defined signals and conditions

Private Enterprise ICS Looks Different from Public ICS

- ICS Framework is Often Scaled Down
- Specific ICS Goals Dominate
- Different Scaling Expectations
- Static/Pre-staffed Role Expectations
- Mutual Aid Not a Major Focus



Have Incident Commander, Will Travel

Uneven and massive usage spikes on services

Resourcing and experience doesn’t necessarily map

Customer patience is not what it used to be

What We Shouldn’t Do

. . . . RIGHT?!

The Warm Blanket Fallacy - *An experienced Incident Commander does not guarantee flawless results in unfamiliar environments*

What We Should Do

Establish a support agreement

What We May Do

Tackling some challenges

Establish a support agreement

Build and hug and love and nurture common ground

What’s an Incident Commander to do?

Tackling some challenges

Establish a support agreement

Build and hug and love and nurture common ground

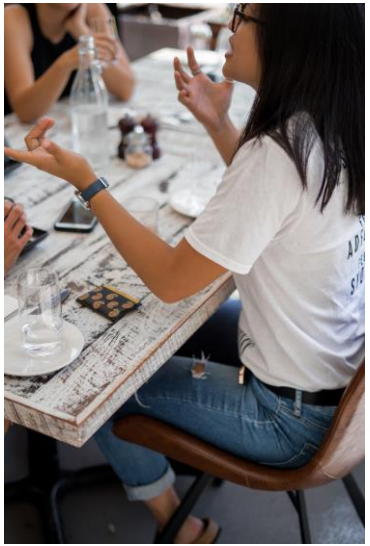
Decentralize command, focus on coordination

Getting Early Learnings

Talk after incidents to help grow more familiar

A significant amount of insight into an incident will come from post analysis

That being said, there are benefits for a response team to talk immediately after the end of an incident, especially when growing familiar with a new organization



Wrapping This All Up

- ICS is a great start, it’s not a packaged solution
- Interorganizational incident response depends on alignment of ICS usage
- Coordination > Command
- Sharing experiences in after action reviews will help grow familiarity in working with each other


THANK YOU