What We Learned

Key Takeaways from the 2018 Ransomware Attack on Colorado Department of Transportation

February – March 2018

Deborah Blyth
Colorado Chief Information Security Officer
Michael Willis
Colorado Director of Emergency Management

Topics

- How It Happened
- What It Did
- Timeline
- How We Responded
  - Business Response
  - Cyber Incident Response
  - Emergency Response
- The Cyber Players
- What We'd Do Differently
- **Key Takeaways**

How It Happened

CDOT brought a virtual server c

Nothing wrong wi

Virtual server conn

Not

Virtu

Brute force attack began the day the server was brought online. Over 40,000 brute force password attempts were made. System was compromised within 48 hours

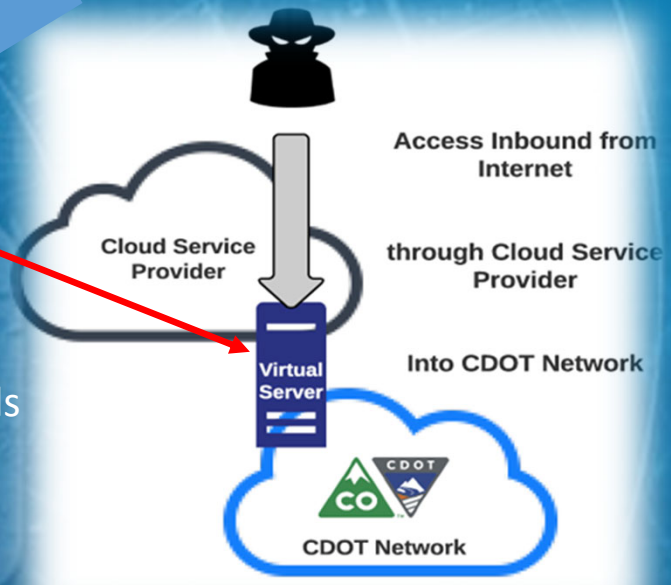
??

t have standard security controls

Uh-oh

tablished as domain administrator account

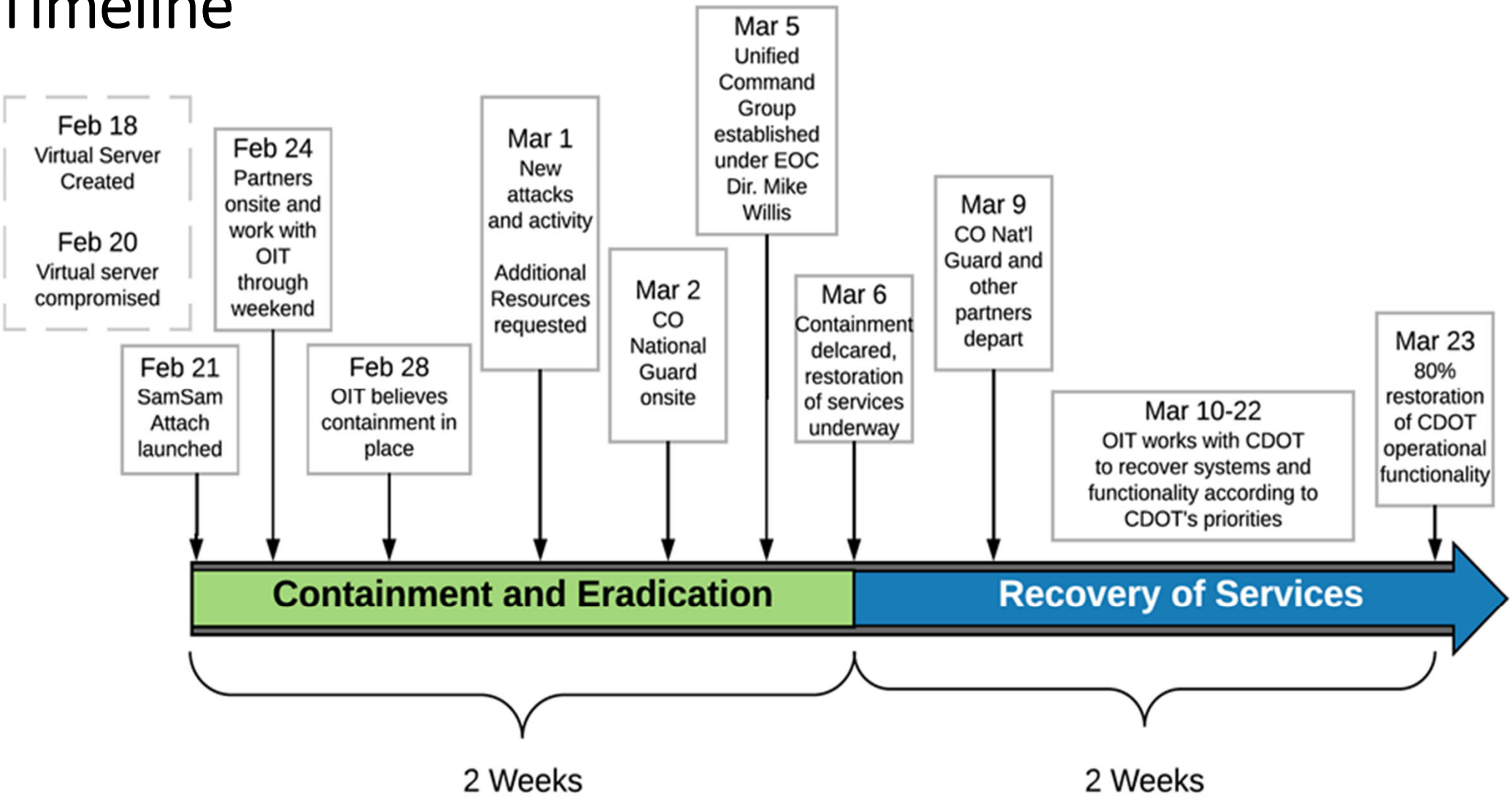
OH #$%&



What It Did

- Equipment
  - 1274 laptops (39%) and 427 desktops (81%)
  - 339 servers
  - 158 databases
  - 154 software applications
  - All VoIP phones
- Consider:
  - How do you pay employees & contractors without the payroll software application?
  - How do you communicate with internal and external stakeholders without email/conference call?
  - What do you tell external contractors when you disconnect them from your network?

Timeline


Feb 18
Virtual Server Created
Feb 20
Virtual server compromised
Feb 21
SamSam Attach launched
Feb 24
Partners onsite and work with OIT through weekend
Feb 28
OIT believes containment in place
Mar 1
New attacks and activity
Additional Resources requested
Mar 2
CO National Guard onsite
Mar 5
Unified Command Group established under EOC Dir. Mike Willis
Mar 6
Containment delcared, restoration of services underway
Mar 9
CO Nat'l Guard and other partners depart
Mar 10-22
OIT works with CDOT to recover systems and functionality according to CDOT's priorities
Mar 23
80% restoration of CDOT operational functionality
Containment and Eradication
Recovery of Services
2 Weeks
2 Weeks

How We Responded

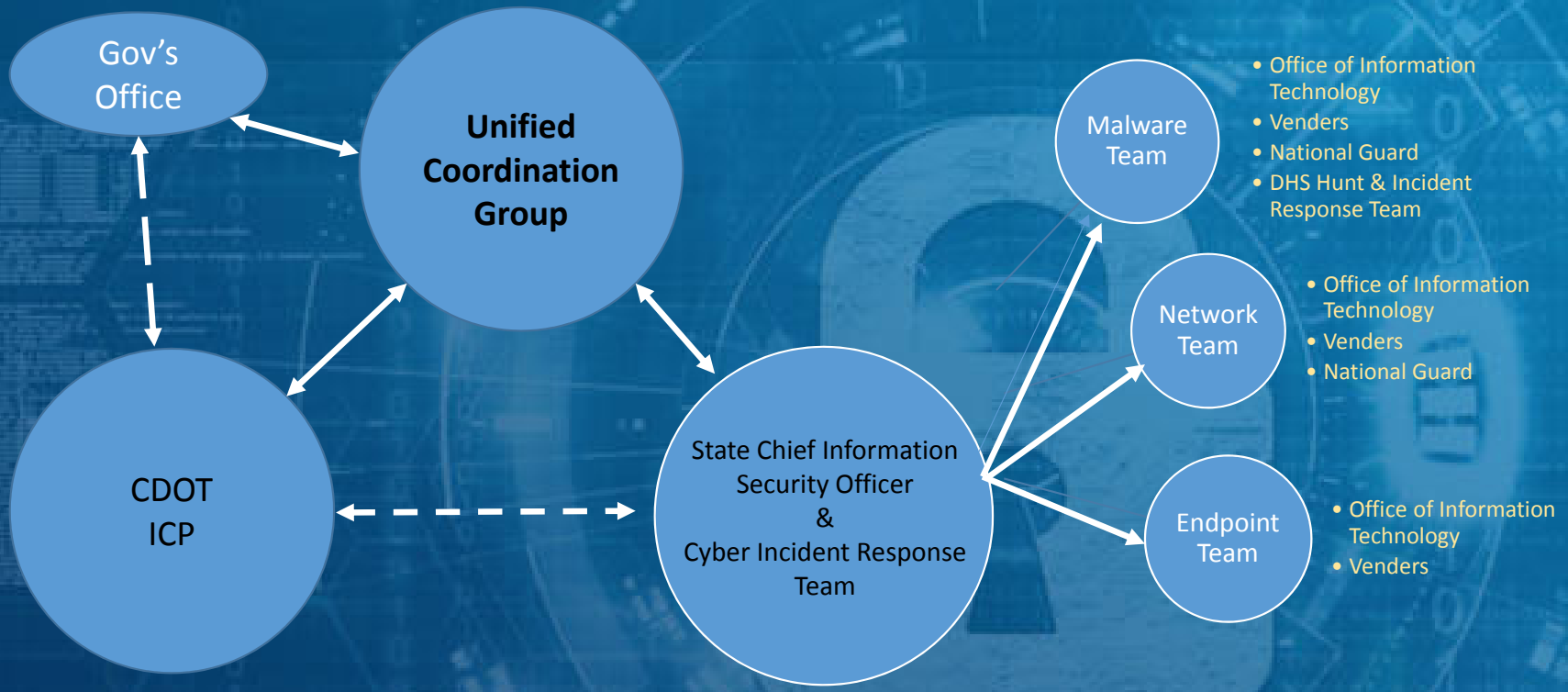
- Business Response
  - Continuity of Operations
    - Internal - employees
    - External – customers
  - Recovery Priorities
    - Operate Financial Systems
    - Protection of Traffic Control Systems
    - Back to Business

- Cyber Incident Response
  - Secure the State Network
    - Contain the attack
    - Secure the Colorado State Network
  - Recovery Priorities
    - Eradicate the malware
    - Secure CDOT
    - Rebuilt CDOT networks

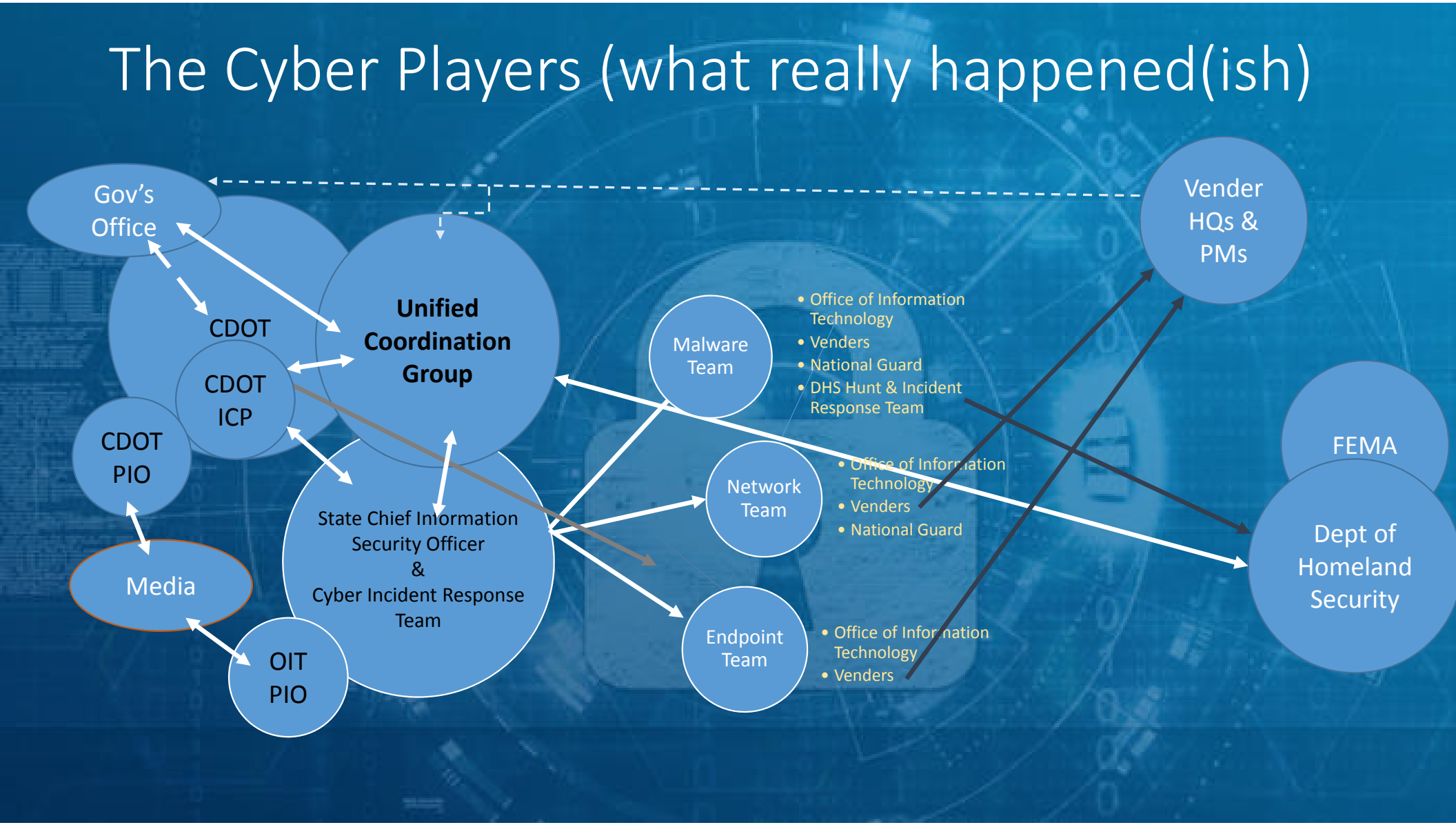
- Emergency Response
  - Understand the Problem Sets
  - Understand the Stakeholder interests
  - Develop common priorities
  - Create unity of effort
  - Referee

Blocks 3 & 4 of ICS 202
Incident Action Plan

The Cyber Players (as designed(ish))



The Cyber Players (what really happened(ish)




Patching Step
[443, 53, 80 On]
Tanium Patching verified
Microsoft
McAfee – ePO servers
SAP Connectivity


Incident Specific Critical Information Requirements:
1. Indications of new infections on the CDOT network
2. Indications that the attack was sponsored by a foreign state
3. Indications the infection has spread beyond the CDOT network
4. Indications of delay to risk of failure for the CDOT COOP
5. Indications that Personally Identifiable Information (PII) or other critical data exposed
6. Indications of information that could negatively impact the interests of the State of Colorado
Daily Rhythm
Critical Information Requirements
Operations


the investigation and gathering evidence
Prioritize handling the incident based on the relevant
impact, recoverability effort, etc.)
Report the incident to the

What We'd Do Differently

- Deploy Incident Command (Unified Command Group) sooner
- Define lanes and organized by tasks sooner
- Clarify lanes and roles with vendors sooner
- Synchronize the operational rhythms sooner (CDOT, Cyber Response, UCG)
- Stop chasing the bad guy sooner

What We'd Do Again

- Coordinate the external message
- Issue an EMAC to rest tired IT personnel
- Call in Office of Emergency Management for logistics coordination
  - How do you feed a roomful of hungry people when they are sick of pizza?
  - How do you keep track of who your responders were?
- Establish priorities early and post priorities on the wall to remind responders of the goals

Key Takeaways

- Define your Cyber Incident Response Team
  - Exactly who does exactly what??
    - Network team
    - Malware team
    - Endpoint team
  - Rehearse (no really – rehearse…)
- Seriously address Cyber in your COOP
  - Holistic approach - not just an IT problem
  - What's at risk? What will you do?
  - CDOT Senior Executive "Our COOP was better suited for a meteor hit than a cyber attack"
- Do cyber response exercises that include Cyber Emergency Management and Business responses
- Mitigate. You mitigate for other risks, so do it for this one
  - Secure backup = mitigation
- It's an incident – act like it!
  - P.S. don't freak out – it's an incident, you've done this before
- Public Information Officers matter!


CONTAINMENT
2018
ERADICATION
RECOVERY
SUSTAIN
CDOT
OIT
CO
CO
HOMELAND SECURITY
PREVENTION
PROTECTION
MITIGATION
RESPONSE
RECOVERY
EMERGENCY MANAGEMENT
SERVING SINCE 1860
CONG
COLORADO NATIONAL GUARD