Cyber Disruption Response Planning Annex

County of San Diego
Office of Emergency Services

Rob Barreras
Senior Emergency Services Coordinator

Cyber Disruption Response Planning Annex

- Provides a **framework for managing** a large scale cyber disruption
- Develops a **Cyber Team** to provide expertise and resources
  - Multidisciplinary – Bringing together IT, Emergency Management, Law Enforcement, and Private Sector
- **Not a tactical plan**. Does **not** supplant any existing plans or procedures.
- Each jurisdiction will utilize the framework to develop their specific response and recovery efforts

Cyber Disruption Response Planning Efforts

- Contract with AECOM (formerly URS) as Subject Matter Experts for development of base Cyber Disruption plan
- **Initial Planning Workshop** – July 2014
- **Emergency Management Institute Virtual Cybersecurity Exercise** – October 2014
- **Annex Review** – January 2015
- **Participants**
  - County (OES, CTO (HP and AT&T), SDSO, LECC)
  - Federal (FBI)
  - Cities

Cyber Disruption Planning

- **Two key lessons learned:**
  - **Information Technology departments and staff can improve their response capability by incorporating Emergency Management staff and principles**, specifically the Incident Command System, in their response actions.
  - **Emergency Management staff and departments are not always aware of their heavy reliance on Information Technology,** nor have they studied the risk profile of critical cyber assets.

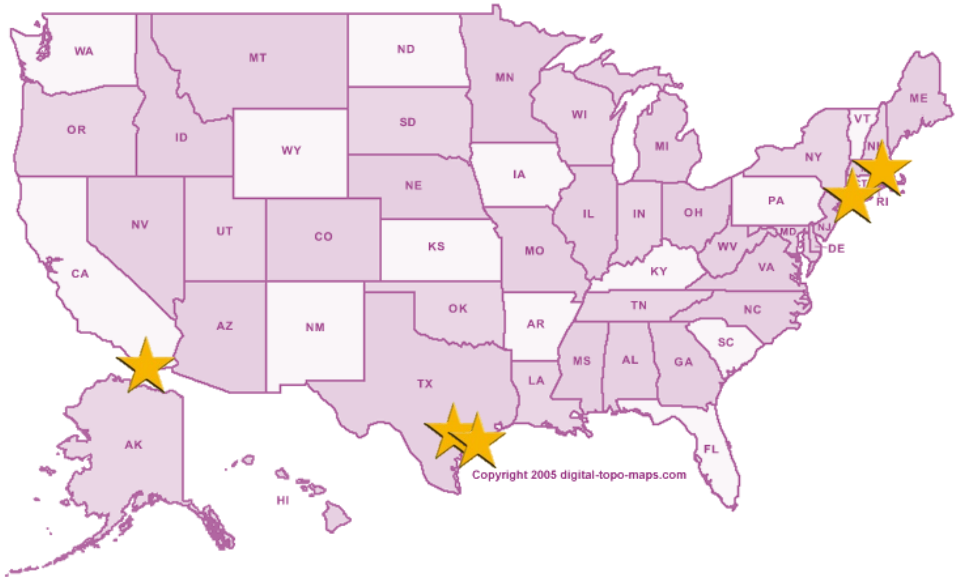
Risk = Probability of Hazard x Degree of Vulnerability

Cyber Disruption Planning

- **Cyber Disruption Response Team**
  - Brings together IT and Emergency Management to create an interdisciplinary response, aimed at improving preparation for, response to, and recovery from significant cyber-disruption events
  - Serves as a panel of experts that can advise the Incident Commander and/or Executive Management during a Disruption Event where the cyber infrastructure is affected, or required

Cyber Disruption Planning

- The Cyber Disruption Response Team concept is being used in a number of jurisdictions across the Country, including:
  - Massachusetts
  - Metro Boston region
  - Rhode Island
  - Houston, TX
  - Harris County, TX
  - Galveston County, TX



…and now San Diego County

Cyber Disruption Response Planning Annex

- San Diego County has developed the **Cyber Disruption Response Planning Annex** for managing a cyber disruption event.

- Cyber Plan consists of 10 Sections:
  - General (Introduction, Purpose & Scope, Assumptions, etc.)
  - Defining the Cyber Disruption Event
  - Outlining Effects-Based Planning
  - Describing Types of Cyber Attacks
  - Cyber Disruption Response Team
  - Communication During a Cyber Disruption Event
  - Plan Maintenance
  - Summary
  - References
  - Appendices

Next Steps

- Finalize the Cyber Disruption Planning Annex – 85%
- Formalize the Cyber Team and engage private sector partners
- Coordinate with CTO, SDSO, HP, and AT&T to focus on County response and recovery efforts
- Capstone 2015 (May 20th) – Full Scale Exercise
  - Activate Cyber Team and Exercise Cyber Plan

Thank You

Rob Barreras
Senior Emergency Services Coordinator
robert.barreras@sdcounty.ca.gov
(858) 527-5889