

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation

CS 4950/5950
Homeland Security &
Cybersecurity

Lesson 38
Disaster Preparation

Rick White, Ph.D.
University of Colorado, Colorado
Springs



1
Esc


1

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation

This module examines what happens in the worst-case scenario precipitated by cyber-attack.



2
Esc

2


UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation

Recall that all disasters advance through four general stages:

1. **Prevent**
2. **Protect**
3. **Respond**
4. **Recover**



3 Esc


3

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Disaster Preparation

- Before a disaster, **Prevention Actions** are taken to reduce the chances of encountering an incident, or mitigating the consequences of future encounters.
- **Protective Actions** are taken to reduce or eliminate a particular threat or hazard.
- After a disaster, **Response Actions** are taken to save lives and protect property.
- **Recovery Actions** seek to alleviate social disruptions caused by the disaster as quickly as possible following the incident.



4 Esc

4




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Disaster Preparation

In this lesson, we examine how the US **Prepares** to **Respond** to disaster precipitated by cyber-attack.



5
Esc

5




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation

- Hope is not a strategy.
- Just as you can't stop a hurricane, you can't stop a determined attacker.
- It's not a matter of "if" but a matter of "when" the next disaster will strike.
- The best time to prepare for disaster is before it strikes.**



6
Esc

6



University of Colorado
Colorado Springs

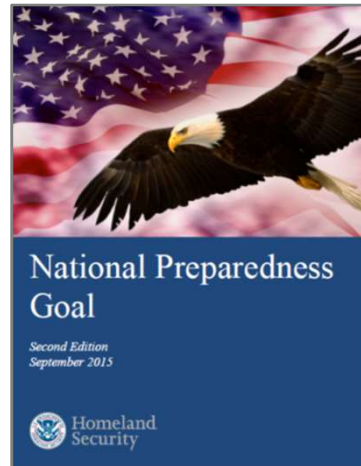
CS4950/5950

Homeland Security & Cybersecurity

Disaster Preparation

National Preparedness Goal

The **National Preparedness Goal** seeks to increase the nation's resilience by building State & Local emergency response capacity.



7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Disaster Preparation

National Preparedness System


The **National Preparedness System** is a continuous improvement process designed to achieve the National Preparedness Goal.



8

Esc

8



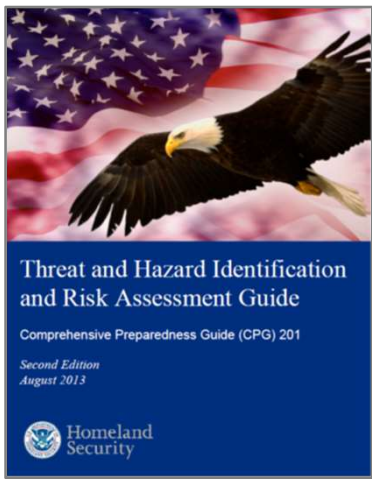
University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation

THIRA


- The National Preparedness System is implemented through THIRA.
- States must use the online **Threat and Hazard Identification and Risk Assessment (THIRA)** program to qualify for annual FEMA **Homeland Security & Grant Programs (HSGPs)**.



9

Esc

9




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation

Identifying & Assessing Risk

- THIRA institutes the first step of the National Preparedness Process, "Identify & Assess Risk".
- Every year, State Emergency Management Officials are required to update their THIRA profile and demonstrate progress towards improved emergency response capability.



10

Esc

10



Disaster Preparation

Estimating Capability Requirements

- Based on the current assessment of their emergency response capabilities, facilitated by THIRA analysis, States may choose to
 - 1) Strengthen existing capabilities, or
 - 2) Build new capabilities.



11

Esc

11



Disaster Preparation

Core Capabilities

- State Emergency Management Officials may choose to strengthen or build capabilities across the four phases of disaster related to 34 different **Core Capabilities** listed in CPG-201 (THIRA).
- The 34 Core Capabilities map to 37 **Target Capabilities** condensed in 2007 from over 1600 unique emergency response tasks compiled in the 2005 **Universal Task List**.

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Forensics and Attribution Intelligence and Information Sharing Interdiction and Disruption Screening, Search, and Detection	Access Control and Identity Verification Cybersecurity Intelligence and Information Sharing Interdiction and Disruption Physical Protective Measures Risk Management for Protection Programs and Activities Screening, Search, and Detection Supply Chain Integrity and Security	Community Resilience Long-term Vulnerability Reduction Risk and Disaster Resilience Assessment Threats and Hazard Identification	Critical Transportation Environmental Response Health and Safety Fatality Management Services Infrastructure Systems Mass Care Services Mass Search and Rescue Operations On-scene Security and Protection Operational Communications Public and Private Services and Resources Public Health and Medical Services Situational Assessment	Economic Recovery Health and Social Services Housing Infrastructure Systems Natural and Cultural Resources

CPG-201 (THIRA) Listed Core Capabilities

12

Esc

12



Disaster Preparation

Building & Sustaining Capabilities

- Every year, State Emergency Management Officials consult County and Municipal governments for their emergency response requirements before updating THIRA.
- **FEMA awards HSGP funds based upon THIRA inputs and politics.**
- HSGP funds are distributed by State Emergency Management Officials to County and Municipal governments to strengthen or build emergency response capabilities by purchasing **equipment, training, or exercises.**



13

Esc

13



Disaster Preparation

Planning to Deliver Capabilities

- State, County, and Municipal agencies prepare for disasters by developing **Emergency Operations Plans (EOPs)**.
- Whether developing new capabilities or strengthening existing ones, Emergency Management agencies must update their EOPs.



14

Esc

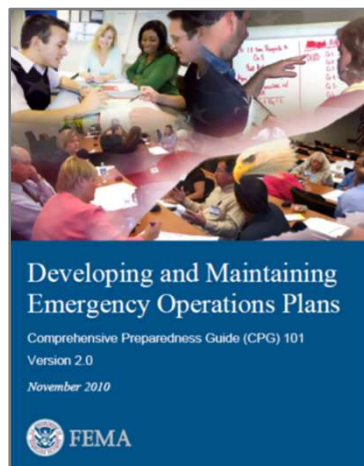
14



Disaster Preparation

Emergency Operations Plans

- FEMA CPG-101 provides guidance on the format and content of EOPs.
- Usually, a different EOP is dedicated to each type of anticipated disaster.
- **CPG-101 advises agencies to prepare for "most likely" disasters.**
- **Natural disasters are most likely.**
- **Manmade disasters are least likely.**
- **Accordingly, specialized capabilities for responding to WMD incidents are not the highest priority for most agencies.**



15

Esc

15



Disaster Preparation

Validating Capabilities

- Whether you purchase equipment or training, the proof that you have improved emergency response capability is testing... exercises.
- DHS developed the **Homeland Security Exercise and Evaluation Program (HSEEP)** to assist communities with conducting emergency management exercises.
- HSEEP exercises can also be sponsored by HSGP grant funding.



16

Esc

16



Disaster Preparation

HSEEP

- HSEEP provides a systematic and common management approach for developing and executing exercises.
- HSEEP helps agencies develop both discussion-based and operation-based exercises.
- **Discussion-based exercises** are designed to introduce new concepts and procedures.
- **Operations-based exercises** are designed to test proficiency with new equipment or procedures.



17

Esc

17



Disaster Preparation

Reviewing & Updating

- The culminating product of HSEEP exercises is the **After-Action Report (AAR)**.
- AARs identify areas of strength, and areas for improvement.
- **All good exercises will reveal areas for improvement.**
- Accordingly, AAR results can provide valid justification for the next round of THIRA updates and HSGP requests.



18

Esc


18

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Disaster Preparation
Identifying & Assessing Risk

And so the cycle continues...



19

Esc


19

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



20

Esc

20