

University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

CWMD & CIP

CS 4950/5950
Homeland Security &
Cybersecurity


Lesson 12
CWMD & CIP

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



¹ Esc

1




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

CWMD & CIP

**What is DHS doing to protect
us from WMD attack or attack
on Critical Infrastructure?**



² Esc

2



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

The Goiania Accident

- 1987, Goiania, Brazil
- A medical device using cesium-137 stolen from abandoned clinic.
- Thieves sell it to a scrap yard.
- The owner's brother scrapes out some cesium and takes it home.
- He sprinkles it on the floor.
- His 6-year-old daughter, attracted by the glow, spread it over her body and sandwich.
- She died a month later and was buried in a lead-lined coffin.
- Four died, 112,000 were examined for exposure.



3

Esc

3



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

DHS Counter WMD

- DHS Counter-WMD Office
- Radiation Portal Monitoring
- BioWatch



4

Esc

4



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Radiation Portal Monitoring

- DHS Domestic Nuclear Detection Office (DNDO).
- Detect and track movement of radioactive agents globally.
- Design & deploy radiation detectors to screen passengers & cargo.
- Key problem with "False Positives"
- 2,734 confirmed intercepts of radioactive material for criminal purposes since 1993.



5

Esc

5



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

BioWatch

- Five killed by Anthrax attack immediately following 9/11.
- In 2003, monitors deployed to 31 cities at cost of \$60 million.
- Again, "False Positive" readings are a problem, plus it takes 36 hours to process results.
- DHS unable to improve technology after 11 years and \$200 million.



6

Esc

6



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

2018 Counter-WMD Strategy

- As part of the Homeland Security Enterprise, DHS teams with DoD, DoS, DoE, and CIA for US CWMD Strategy.
- DHS leads CWMD efforts highlighted in red (at right).

2018 US CWMD Strategy

1. **Deny** WMD to terrorists.
2. **Detect & Defeat** WMD plots.
3. **Degrade** WMD capabilities.
4. **Deter** WMD terrorism.
5. **Globalize** WMD fight.
6. **Strengthen** WMD defenses.
7. **Enhance** WMD response.
8. **Avoid** technological surprise.

7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

CWMD vs. CIP

- Essentially, CWMD Strategy is about keeping WMD agents out of the hands of people the US doesn't want to have them.
- By comparison, CIP is more difficult, because you can't separate people from critical infrastructure.



8

Esc

8



Critical Infrastructure Protection

- CIP began in May 1998 when President Clinton signed PDD-63 directing protection from “physical and virtual” attacks.
- PDD-63 prompted by 1997 Presidential Commission Report citing future possibility of cyber-attack.
- Report commissioned as a result of 1995 Tokyo Subway attacks.



9

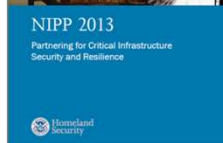
Esc

9



NIPP

- PDD-63 did too little too late to prevent 9/11 attacks.
- 2002 Homeland Security Act made CIP a core DHS mission, together with Cybersecurity.
- **2002 Homeland Security Act directed DHS to draft what became the National Infrastructure Protection Plan.**
- Three separate plans have since been released.



10

Esc

10

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Critical Infrastructure Protection

- NIPP essentially copied process identified in PDD-63.
- Federal agencies worked with industry to develop Sector Specific Plans (SSPs).
- SSPs follows 5-step Risk Management Framework to incrementally reduce vulnerability to attack.**
- One SSP for each of the 16 infrastructure sectors identified in 2011 PPD-21.

11 Esc

11

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

RMF Step 1

- In Step 1, DHS works with industry representatives to **establish infrastructure protection goals and document these in the Sector-Specific Plans.**
- The Sector-Specific Plans are supposed to be updated every four years; **the most recent public versions were released in 2016.**

12 Esc

12

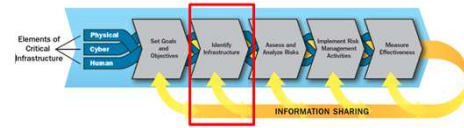


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


RMF Step 2

- In Step 2, the DHS works with State governments to annually **update a list of critical infrastructure** under the **National Critical Infrastructure Prioritization Program**.
- The NCIPP is protected information not releasable to the public.



13
Esc

13




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

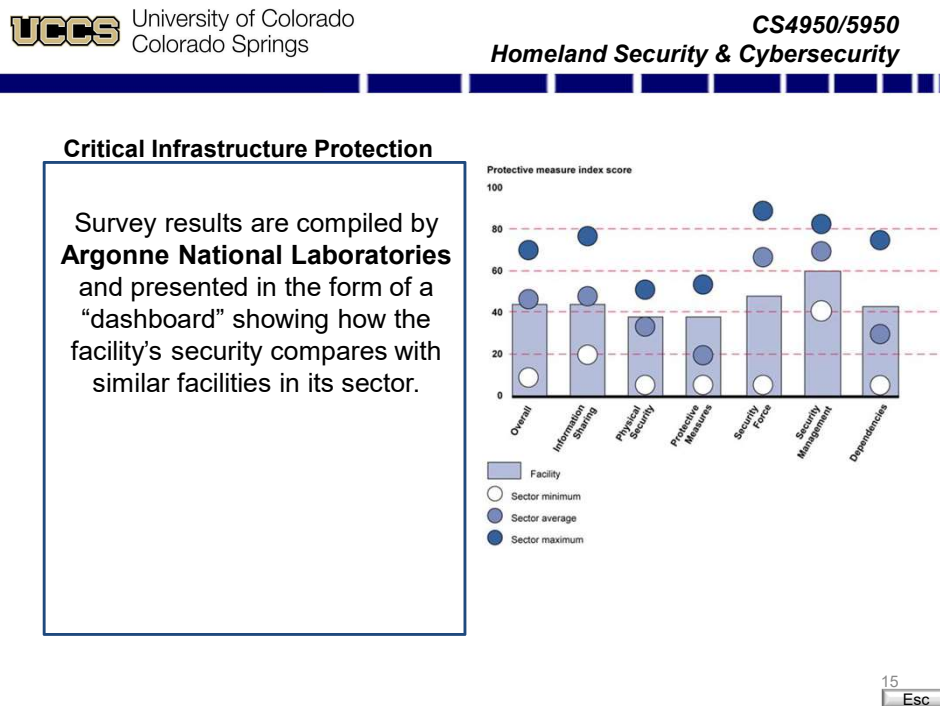
RMF Step 3

- For Step 3, **DHS Protective Security Advisors** will **conduct Site Assistance Visits and complete Security Surveys and Resilience Assessments** at the request of infrastructure owners/operators.
- The **Infrastructure Survey Tool** employed by PSAs consists of 1500 questions examining both physical and cyber security measures.

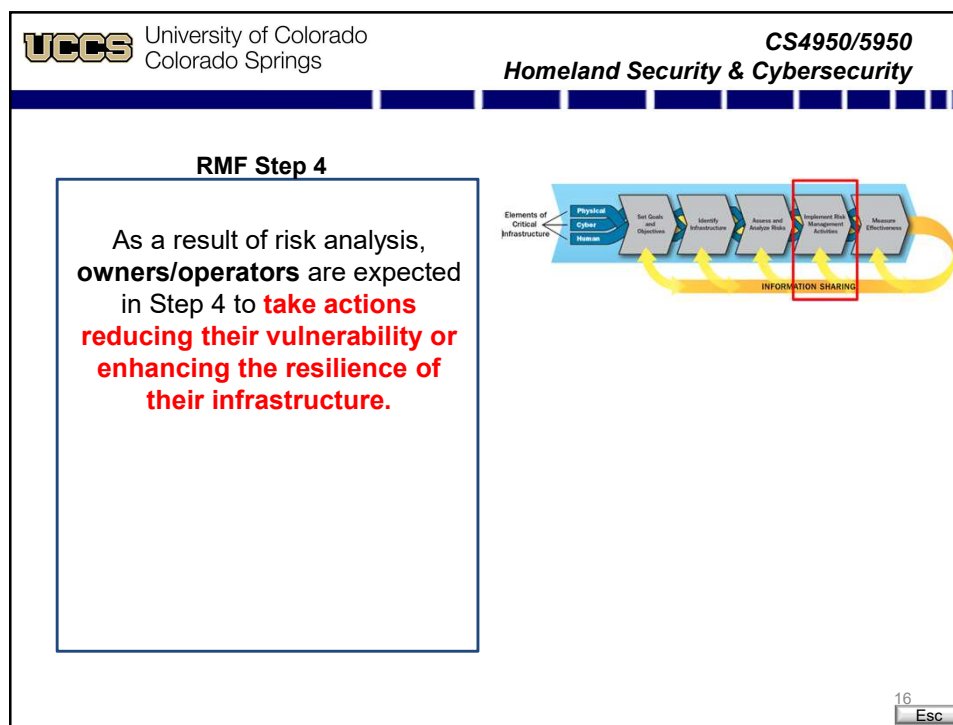


14
Esc


14



15



16




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Critical Infrastructure Protection

- Owners/operators are willing to take on increased security and resilience subject to costs.
- **Market forces and regulatory restrictions constrain what measures are practical.**
- **Federal funds administered under the DHS Homeland Security Grant Program, and other such programs administered by FEMA help State and Local governments compensate for what measures industry can't implement.**



17
Esc

17




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


RMF Step 5

- Step 5, “Measure Effectiveness”, is meant to **provide a means of assessing progress towards protective goals set out in the Sector-Specific Plans.**
- To date, DHS has been unable to develop a uniform set of metrics to measure progress towards improved security and resilience.



18
Esc

18



University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Critical Infrastructure Protection

- In fact, every step of the Risk Management Framework is fraught with problems, and the process is not nearly as coherent as described.**
- Perhaps one reason is that the process is entirely voluntary on the part of industry, and for both legal and business reasons, industry does not entirely trust government.

RMF Problems

Step 1: Reluctance to reveal proprietary data.

Step 2: Multiple databases with incomplete and questionable assets.


Step 3: No uniform analysis for comparing risks across assets and sectors.

Step 4: No direct funding to private industry.

Step 5: No established metric for guiding national strategy.

19
 Esc

19

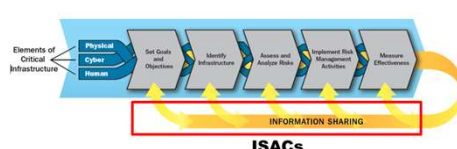


University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Critical Infrastructure Protection

- Accordingly, DHS has also tried to help industry help itself by establishing sector-related **Information Sharing and Analysis Centers.**
- These sector-related ISACs are managed by industry and provide a **central clearing house for reporting problems and seeking solutions.**



20
 Esc

20



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Critical Infrastructure Protection

- In addition to working with industry through the National Infrastructure Protection Plan, DHS manages the **National Infrastructure Coordinating Center** which maintains continuous watch on the status of nation's infrastructure.
- **If something happens requiring Federal support, the NICC will perform the necessary coordination.**



21

Esc

21



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Summary

- Despite appearances, DHS plays a very small role in protecting the US from WMD attack and attack on CI.
- DHS is primarily limited in CWMD by its ability to accurately track WMD agents.
- DHS is primarily limited in CIP by its lack of control, **and more importantly, the lack of effective security measures.**



22

Esc


22

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



23

Esc