University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

DHS Cyber Response

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 34
DHS Cyber Response

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

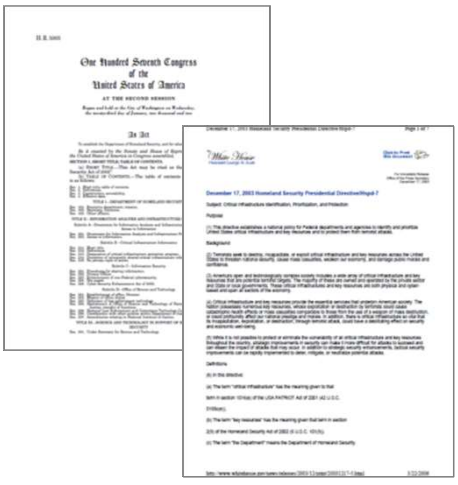
1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

DHS Cyber Missions

- **2002 Homeland Security Act**
  - Analysis & Warning of Threats
  - Crisis Management Support
  - Technical Assistance
- **2003 HSPD-7**
  - Facilitate Collaboration
  - Information Sharing
  - Vulnerability Reduction
  - Mitigation
  - National Recovery

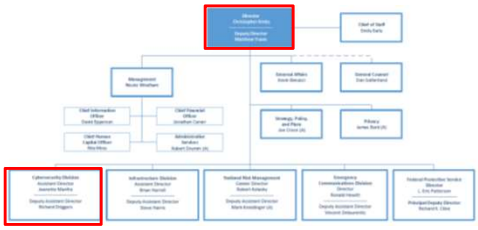

One Hundred Seventh Congress
of the
United States of America

2

DHS Cyber Organization

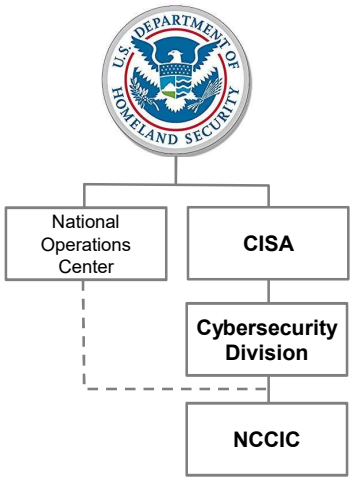
- Cybersecurity & Infrastructure Security Agency*
- **Cybersecurity Division.**

*In October 2018, the Senate passed legislation renaming the National Protection and Programs Directorate (NPPD) the Cybersecurity and Infrastructure Security Agency.



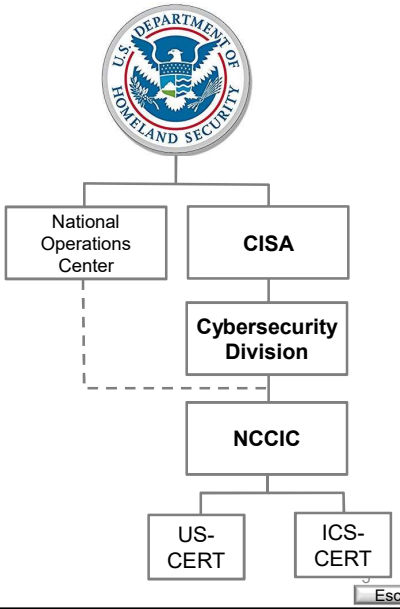
Cybersecurity

CISA Cybersecurity Division stands watch over cyber attack from the **National Cybersecurity and Communications Integration Center.**



Cybersecurity

- **NCCIC** is a 24-hour operations center ready to coordinate a national cyber incident response.
- Among its assets, the NCCIC can call upon the **US-CERT** and **ICS-CERT**.



Esc

5

Cybersecurity

The **US Computer Emergency Readiness Team** at Carnegie Melon University, Pennsylvania, works with product developers to remove security vulnerabilities in their software, and **provides a clearinghouse for gathering threat data and disseminating alerts and countermeasures.**

6

Esc

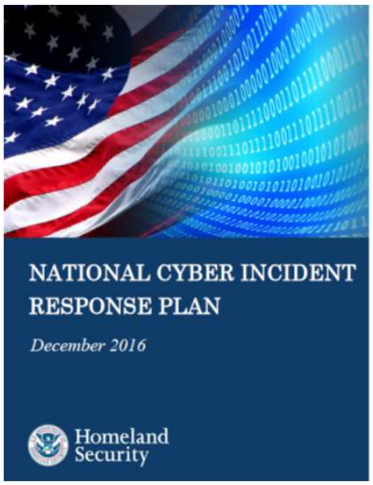
6

Cybersecurity

The **Industrial Control Systems Cyber Emergency Response Team** performs similar functions to US-CERT for industrial control systems, but also has ready an **emergency response team that can deploy upon request** to help resolve a specific cyber incident.

Cyber Incident Response Plan

- Developed based on direction in 2016 **PPD-41**, US Cyber Incident Coordination.
- Articulates roles, responsibilities, capabilities, and coordinating structures for responding to significant cyber incidents.



Cyber Incident Severity

- **Cyber Incident.** Essentially any type of cyber attack.
- **Significant Cyber Incident.** A cyber incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

9

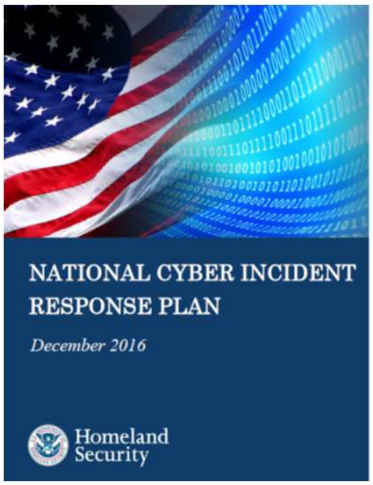
Esc

9

University of Colorado Colorado Springs
CS4950/5950
Homeland Security & Cybersecurity

Cyber Incident Responsibilities

- **DoJ.** Lead agency for **threat response** to a significant cyber incident.
  - Find & arrest criminal culprit.
- **DHS.** Lead agency for **asset response** to a significant cyber incident.
  - Stop the hurt from hurting.



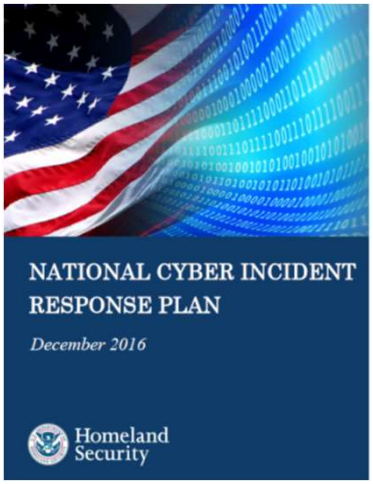
10

Esc

10

DHS Asset Response

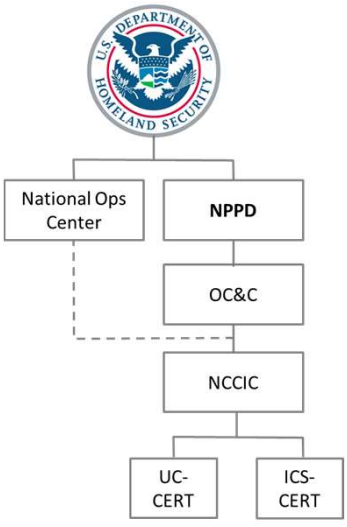
- Lend Technical Assistance
  - Protect, Mitigate, Diminish
- Identify Other Potential Victims
- Assess Potential Risks
- Facilitate Information Sharing
- Advise on Federal Resources



11

ICS-CERT

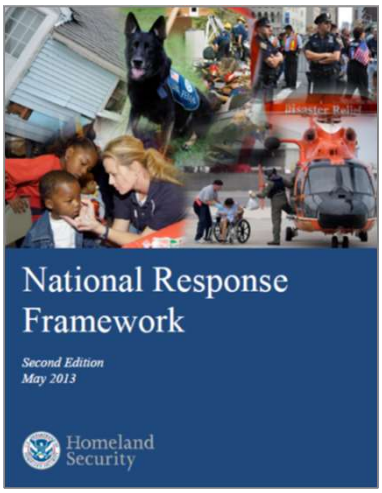
- As we learned in Lesson 10, ICS-CERT maintains deployable teams ready to respond upon request.
- **The problem is they wouldn't be familiar with your site installation, and there may not be enough of them to help.**



12

DHS Cyber Response

- Even so, as with all government support, you probably **shouldn't expect any assistance to arrive on scene before 72-hours** after you place the call.
- It then begs the question whether the support **might be too little too late.**



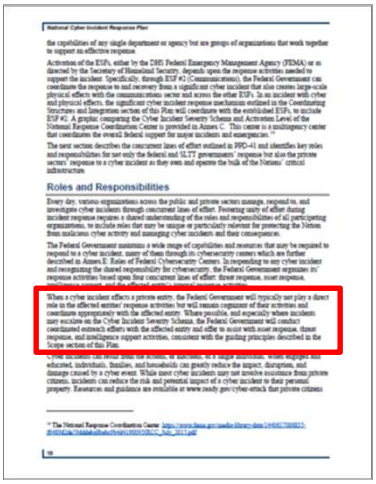
13

Esc

13

WTF?

"**When a cyber incident affects a private entity, the Federal Government will typically not play a direct role in the affected entities' response activities** but will remain cognizant of their activities and coordinate appropriately with the affected entity."


Roles and Responsibilities

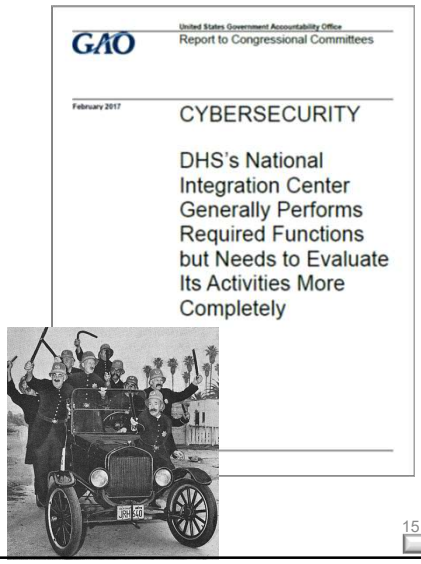
14

Esc

14

2017 GAO Report on NCCIC

- NCCIC **had not established measures or procedures** for providing timely technical assistance, risk management, or other incident response capabilities.
- NCCIC officials **unable to track and consolidate cyber incidents** reported to them.
- NCCIC **doesn't have current contact information** for all owners and operators of the most critical cyber infrastructure assets.



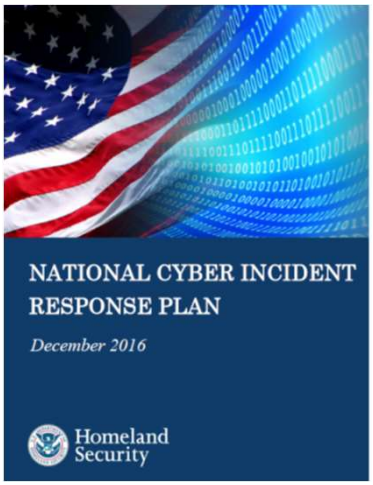
15

Esc

15

Collateral Support

- Industry Helping Industry:
  - **Information Sharing and Analysis Centers**
  - Information Sharing and Analysis Organizations



16

Esc

16

Industry-Helping-Industry

- The **obvious advantage of working within your industry is that you are more likely to have greater interoperability of skills and equipment** because you share common practices.
- **The biggest drawback to working within your industry is that the best qualified responders may be your competitors.**
- This inherent conflict works against collaborative planning for collective incident response.

Collateral Support

- Advantage: Interoperability
- Disadvantage: Competitor

17

DHS Cyber Response

- Understanding, therefore, that cybersecurity is about risk management, it's reasonable to say **it's not a matter of "if" but "when" you're going to get hacked.**
- **The question is what do you do?**

18

DHS Cyber Response

Going back to our working definition of homeland security, "Safeguarding the United States from domestic catastrophic destruction", we know that "**safeguarding" entails actions across all phases of disaster, and that they are prevent, protect, respond, and recover.**

19

DHS Cyber Response

- Actions to prevent and protect from catastrophic destruction are generally taken before an incident occurs.
- Actions to respond and recover only become necessary after an incident occurs.

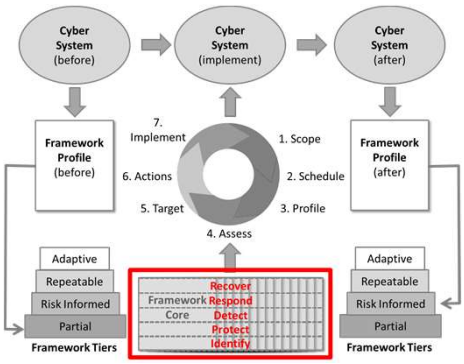
20

DHS Cyber Response

- Accordingly, if we write these actions on a timeline representing some incident indicated by the word "boom", we can say that prevent and protect actions occur to the "**left of the boom"**, while respond and recover actions occur to the **"right of the boom".**
- This is just an easier way of understanding the dynamics of catastrophes, the same way our working definition of homeland security makes it easier to understand the official definitions of homeland security.

DHS Cyber Response

- Anyway, if you look back at the cybersecurity models we studied in Part 2 and Part 3, you will notice they include actions both to the left and right of the "boom".
- **Just because you've succumbed to cyber attack doesn't mean your cybersecurity has failed.**



DHS Cyber Response

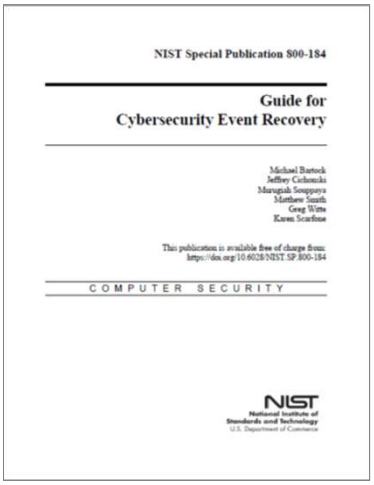
- The success of your cybersecurity strategy still depends on **how quickly you can respond and recover from cyber attack.**
- This is where those investments, possibly harder to justify to management, prove their worth hundreds of times over.

DHS Cyber Response

- Obviously, the quicker you can recover and return to normal operations, the smaller the impact the cyber attack will have on your mission.
- **The ability to quickly recover and return to normalcy is termed "resiliency".**

NIST 800-184: Appendix A Checklist

1. Preparing for Recovery
2. Tactical Recovery
   1. Initiation
   2. Execution
   3. Termination
3. Strategic Recovery
   1. Initiation
   2. Execution
   3. Termination


NIST Special Publication 800-184

Guide for
Cybersecurity Event Recovery

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Matthew Smith
Greg Witte
Karen Scarfone

This publication is available free of charge from:
http://dx.org/10.6028/NIST.SP.800-184

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DHS Cybersecurity

In the end, your first and last line of cyber defense is your own IT support.

Conclusion

Questions?