Work partly funded by the National Science Foundation Grant #1303269.
PIs: Sumita Mishra, R. K. Raj, C. Romanowski, and J. Schneider

Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

CSCI 455: Principles of Computer Security

Set 06:

Critical Infrastructure Protection (CIP) and Computer Security and Privacy

Video

- Department of Homeland Security
  - National Infrastructure Protection Plan
    - http://www.dhs.gov/video/national-infrastructure-protection-plan

What is Critical Infrastructure?

- Definition
  - Systems and assets so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters
- Physical or Virtual

CIP Drivers

WAR

Natural Disaster

Dependencies

Response Plans

Cyber Attacks

Terrorism

Globalization

Regulations

What happens when this happens?

http://images.nationalgeographic.com/wpf/media-live/photos/000/332/cache/japan-earthquake-tsunami-nuclear-unforgettable-pictures-ship_33287_600x450.jpg

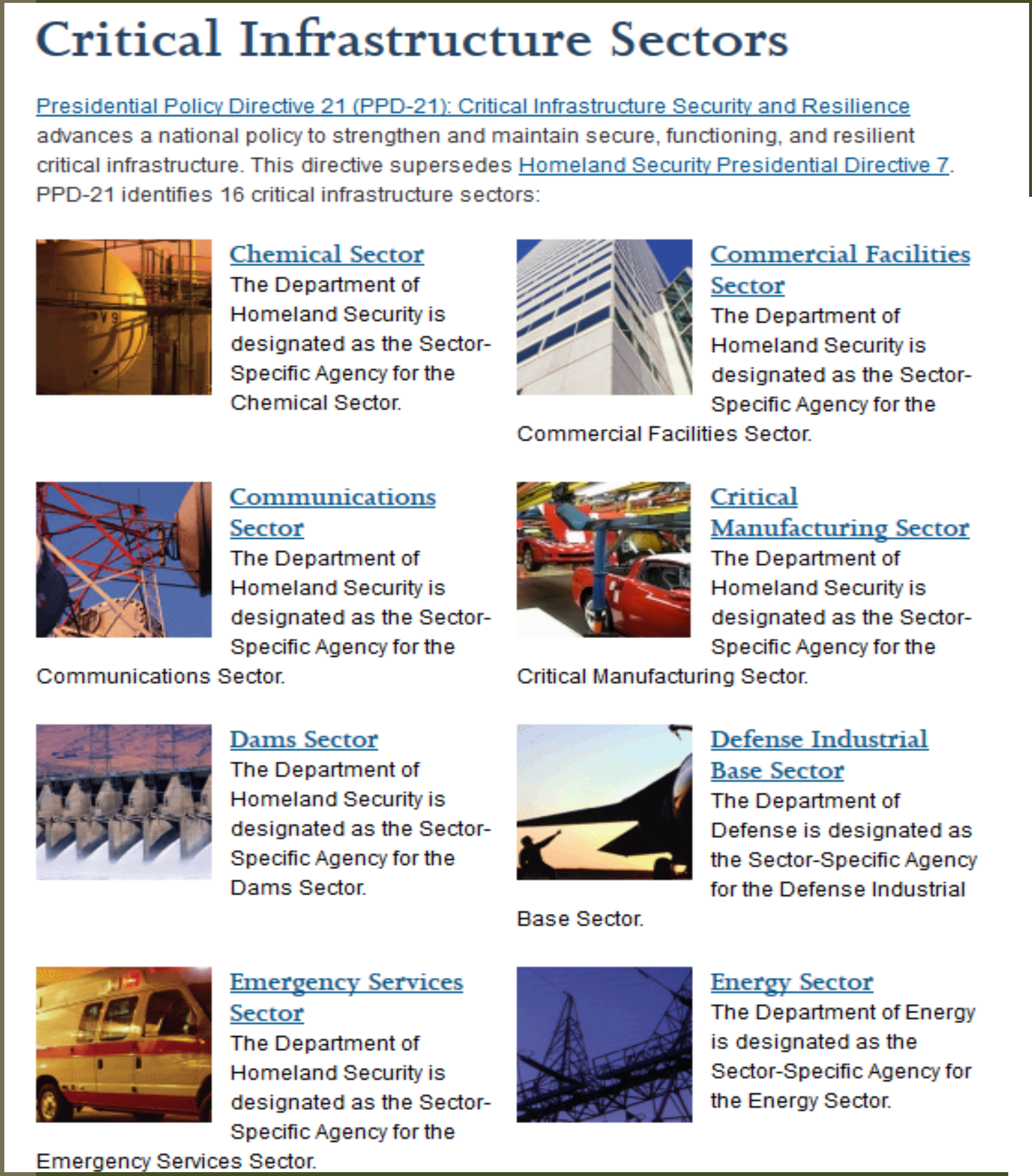
p://a.abcnews.com/images/Polit /ht_gjs-wtc014_100205_ssv.jpg

http://www.esri.com/news/arcnews/winter0304articles/winter0304gifs/p20p1-lg.jpg

http://media.nola.com/hurricane_katrina/photo/8778913-small.jpg

http://www.popsugar.com/celebrity/Snowstorm-Buffalo-NY-November-2014-Pictures-36138701

http://www.classicbuffalo.com/images/Blizzard77Roof.jpg



Critical Infrastructure Sectors

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Communications Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Communications Sector.

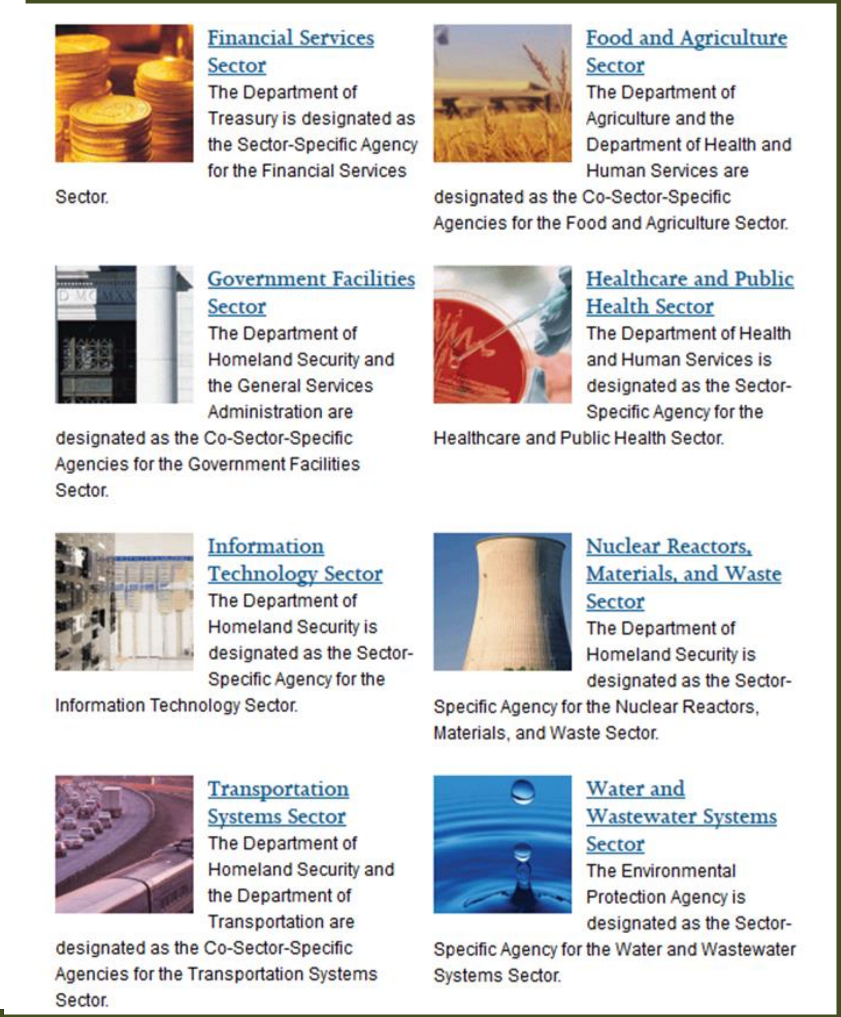
Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector.

Defense Industrial Base Sector
The Department of Defense is designated as the Sector-Specific Agency for the Defense Industrial Base Sector.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector.

Energy Sector
The Department of Energy is designated as the Sector-Specific Agency for the Energy Sector.



Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

CIP THEMES

- Physical
- Human
- Cyber

Physical

- Examples
  - Buildings
  - Equipment
    - Computer rooms and centers, including power supplies, air-conditioning systems, and backup generators
  - Telecommunication equipment include landline phones, including those running on electricity
  - Peripherals – printers, cameras, microphones
  - Networking equipment such as routers, switches, access points
  - Locks on doors

- Other Examples
  - Dams,
  - Water Resources
  - Electrical System – Cyber-Physical
    - Smart Grid
      - Sensor Networks play a key rol

Human

- Examples
  - Unintended exposures
    - Your Facebook page
    - Where is your phone? Your laptop?
  - Is your sensitive data encrypted?
  - Passwords
  - What are consequences of losing that USB drive?
- Building human firewalls
- Some other examples
  - Critical People

Cyber

- Computing hardware
  - Operating systems, application software, middleware
- Secure information management
  - Database management systems, secure networking, privacy preserving data mining, …
- Secure and defense control systems
  - Supervisory Control and Data Acquisition (SCADA) systems
- Communication systems
  - Email, text, phone (landline, cell, VOIP)
- Others?

CIP Conceptual Framework

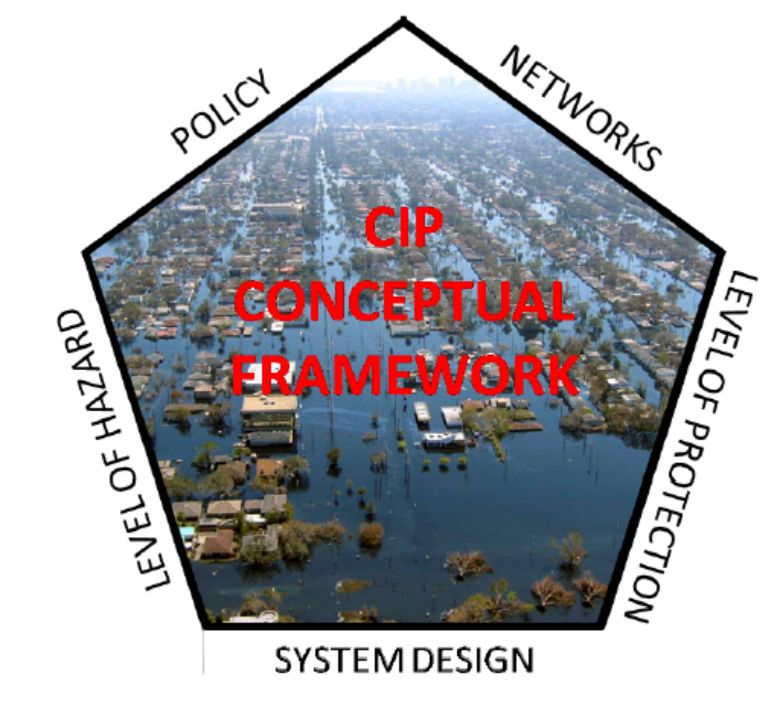
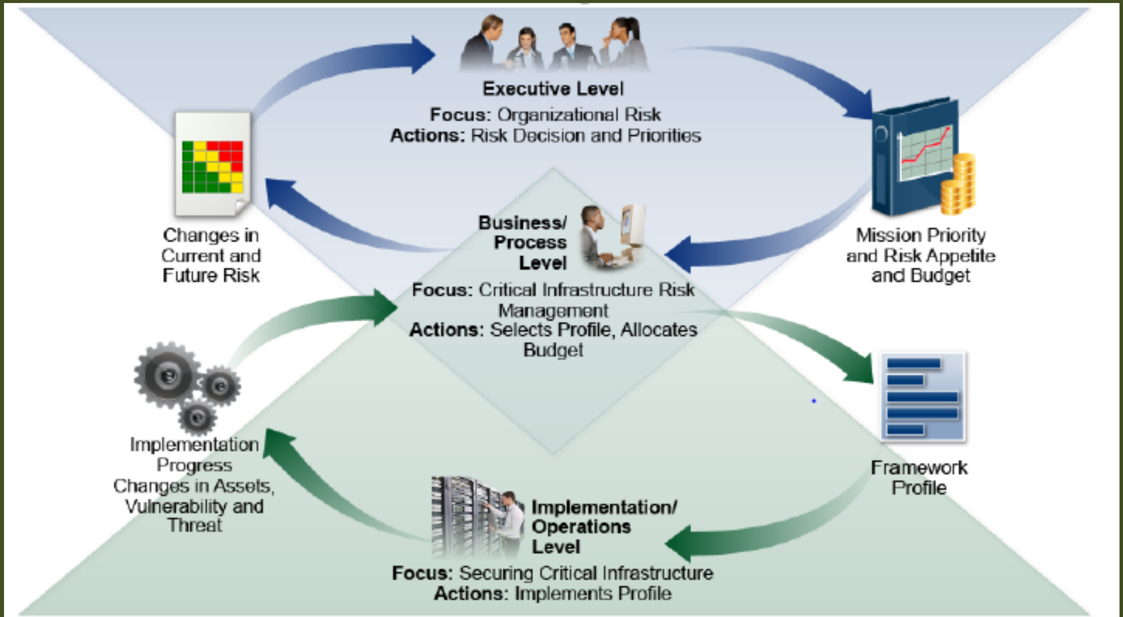


Figure and text from Steven Hart and Jim Ramsay, "A Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses"

- Framework as Objectives
  - Explain national strategies and policies on infrastructure protection
  - Identify critical components of a complex infrastructure network
  - Describe the All Hazards Environment for those critical components
  - Specify the level of protection or resiliency for those critical components
  - Describe systems design concepts to achieve the desired protection and resiliency

Risk Management

- Ongoing process of identifying, assessing, and responding to risk
- To manage risk, organizations must understand likelihood of an event and its resulting impact. With this information, organizations can determine acceptable level of risk for delivery of services, which defines their risk tolerance.



Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Figure from the NIST Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, Feb 12 2014

Risk Management: Planning

- Identity risks, vulnerabilities, and compose response plan
  - Shore up or negate vulnerabilities to limit risks
    - Vulnerabilities are internal
    - Risks are internal and external
- Protect and preserve critical operations
  - Virtual and physical attributes
  - Determine alternatives
- Provide for detection or reporting processes for occurrence
  - The three As
    - Anomalies
    - Awareness
    - Access

Risk Management: During

- Activate plan
  - Incident command, technical experts, assessment of scope and damage
  - CIP response needs to be well planned out and quick
- Communicate
  - Determine scope of communications
  - Levels of information based upon possible impact and capability

- Mitigate
  - Prevent expansion of event
  - Minimize its effects
  - Eradicate the event

Consider these events

- Natural disasters such as hurricanes or floods
- Man-made disasters such as terrorist attacks
- Other emergencies such as epidemics or power outages

Risk Management: During (continued)

- Levels of responsibility
  - You
  - Your family
  - Town/city government
  - County government
  - State government
  - Federal government
- Where do these fit in?
  - Private companies
  - Non-profits
  - Volunteers

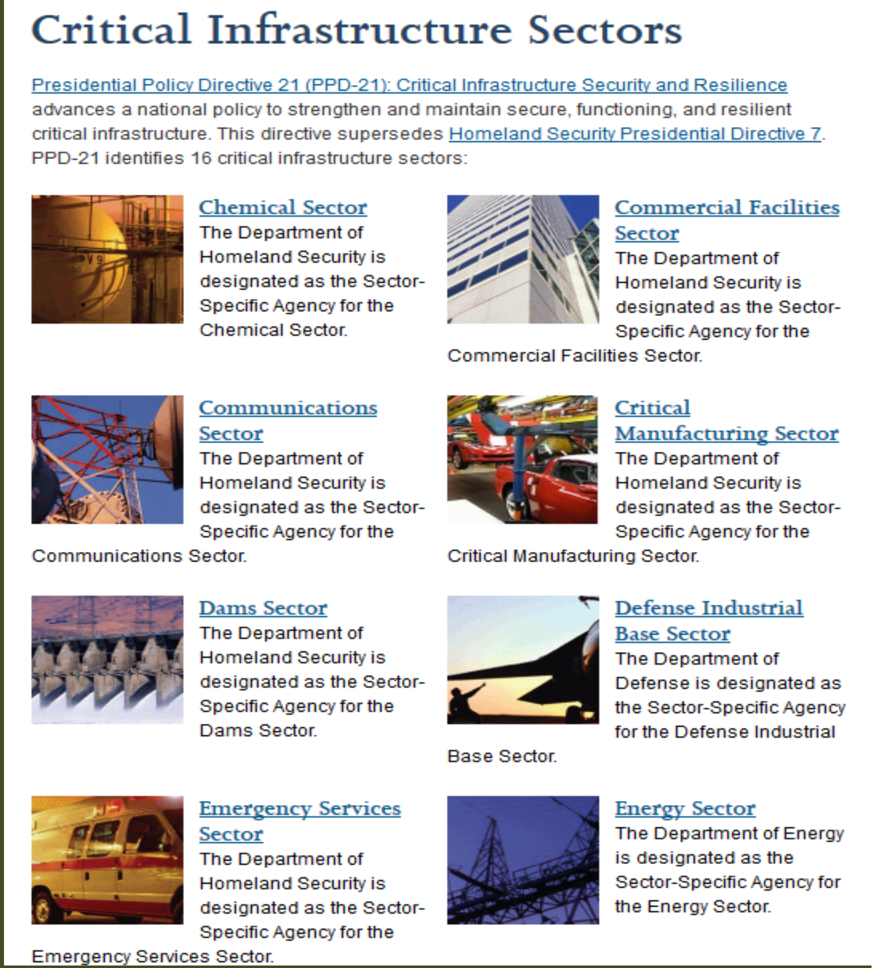
- “Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets.”
  - http://www.gao.gov/products/GAO-07-39

Risk Management: After

- Recovery
  - Communications
  - System fixes
  - Conduct action assessment
  - Revise both risk plan and operations plan

Computing and Data Management Role in Critical Infrastructure Protection

Role of Computing in CIP: Discussion



Critical Infrastructure Sectors

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Communications Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Communications Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector.

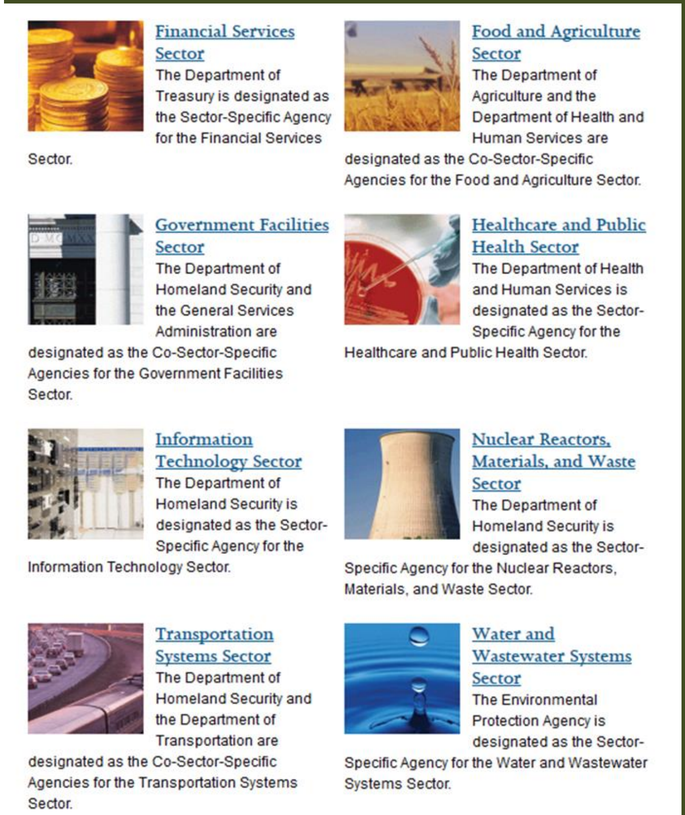
Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Defense Industrial Base Sector
The Department of Defense is designated as the Sector-Specific Agency for the Defense Industrial Base Sector.

Energy Sector
The Department of Energy is designated as the Sector-Specific Agency for the Energy Sector.



Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Database Systems in CIP

- Two major roles
  - DBMSs form part of critical infrastructure in all 16 CI sectors
    - Why?
  - DBMSs help to support CIP
    - PCII – Protected Critical Infrastructure Information Program
    - ACAMS – Automated Critical Assets Management System
    - CVI – Chemical-terrorism Vulnerability Information Program

Protected Critical Infrastructure Information (PCII) Program

- Enhances voluntary information sharing among infrastructure owners/operators & government
- Data confidentiality is assured!
- PCII data is used to …
  - Analyze and secure critical infrastructure and protected systems
  - Identify vulnerabilities and develop risk assessments
  - Enhance recovery preparedness measures

http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program

ACAMS

- Automated Critical Assets Management System
  - Provides a secure, online database management and analysis platform
    - Owners/operators to play active role in infrastructure protection programs by maintaining accuracy of their asset's data
    - Collection/management/analysis of critical infrastructure asset data
    - One-click access to critical asset data to for emergency response
  - Development of a variety of pre- and post-incident response plans for strategic and operational planners and tactical commanders
  - Effective information sharing & collaboration across agencies
  - …

http://www.dhs.gov/automated-critical-asset-management-system-acams http://www.dhs.gov/chemical-terrorism-vulnerability-information

CVI

- Chemical-terrorism Vulnerability Information Program
  - Information protection regime to protect from inappropriate public disclosure any information developed or submitted pursuant to Section 550
  - Includes information developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation
  - Chemical facilities expect that information provided to DHS will be protected from public disclosure or misuse
- DHS expects individuals in possession of CVI to safeguard it with equal care
- Ensure sensitive information about the Nation's high-risk chemical facilities is safeguarded

Information Sharing: Data and Computing Security/Privacy

- Between CIP Owners and Operational Staff
  - Is PCII sufficient?
  - Has it been found to be acceptable?
- Who owns most of US CIP?
- Issues of data security and privacy
  - Data security in information sharing?
  - Data privacy in information sharing?

References: CIP In General

- Executive Order -- Improving Critical Infrastructure Cybersecurity, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed Nov 12 2014).
- Presidential Policy Directive -- Critical Infrastructure Security and Resilience, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed Nov 12 2014).
- National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (accessed Nov 12 2014).
- Steven Hart and Jim Ramsay, "A Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses," Homeland Security Affairs Journal, Vol VII, 2011. http://www.hsaj.org/?fullarticle=7.1.11 (accessed Nov 12 2014.

References: Our Work

- Schneider, J., Romanowski, C. and Stein, K. "Decision making to support local emergency preparation, response, and recovery," in IEEE Conference on Technologies for Homeland Security (HST '13), Boston, 2013.
- C. Romanowski, R. K. Raj, J. Schneider, S. Mishra, V. Shivshankar, S. Ayengar and F. Cueva, Regional Response to Large-scale Emergency Events: Building on Historical Data,. International Journal of Critical Infrastructure Protection, Volume 11, December 2015.
- Romanowski, C., Schneider, J., Mishra, S., Raj, R.K., Rosario, R., Stein, K. and Solanki, B. Response and Recovery: A quantitative approach to emergency management,. 2016 IEEE International Conference on Technologies for Homeland Security (IEEE HST 2016), to appear.
- Romanowski, C., Mishra, S., Raj, R.K., Howles, T. and Schneider, J. .Information Management and Decision Support in Critical Infrastructure Emergencies at the Local Level,. IEEE Conference on Technologies for Homeland Security (HST .13), Boston, Nov 2013.
- Mishra, S., Romanowski, C., Raj, R.K., Howles, T. and Schneider, J. (2013). .A Curricular Framework for Critical Infrastructure Protection Education for Engineering, Technology and Computing Majors. Proc. of 2013 Frontiers in Education Conference, Oklahoma City, OK.
- Alshehri, S., Mishra S. and Raj, R.K. .Insider Threats and Access Control in e-Health Systems.16th IEEE International Conference on e-Health Networking, Applications and Services (IEEE Healthcom 2014), Natal, Brazil. Oct 2014.
- McNett, A., D.J. Dates, D.J. and S. Mishra, S. (2015). Security and Education: Collaborative Modular Approach to Embedding Security Concepts. Innovations: The League for Innovation in the Community College Annual Conference (Innovations .15), Boston, MA.
- Mishra, S., Raj, R., Romanowski, C., Schneider, J., and Critelli, A. (2015). On building cybersecurity expertise in critical infrastructure protection. IEEE Conference on Technologies for Homeland Security (HST '15), Waltham, MA.
- Schneider, J., Romanowski, C. J., Raj, R. K., Mishra S., and Stein, K. .Measurement of locality specific resilience: an operational model,. 2015 IEEE International Conference on Technologies for Homeland Security (IEEE HST 2015), Waltham, MA. April 2015.

Paper Summary

Carol Romanowski, Rajendra Raj, Jennifer Schneider, Sumita Mishra, Bernard Brooks, Jessica Pardee, Bharat Bhole and Nikolaus Robalino, "The Community as Responder: A Multidisciplinary Predictive Model for Managing Critical Infrastructure Disruptions," Tenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Arlington, Virginia. March 2016.

Project Motivation

- Residents cleared 4-7 feet of snow from their neighborhood streets before city and county plows could reach their area
  - If such capacity was known to be available, functional and operational, area emergency managers could have assigned resources more effectively
- But at present, such community resource systems
  - Underutilized and often actively discouraged by professional responders

How can these community resources be factored in improve overall response efficacy?

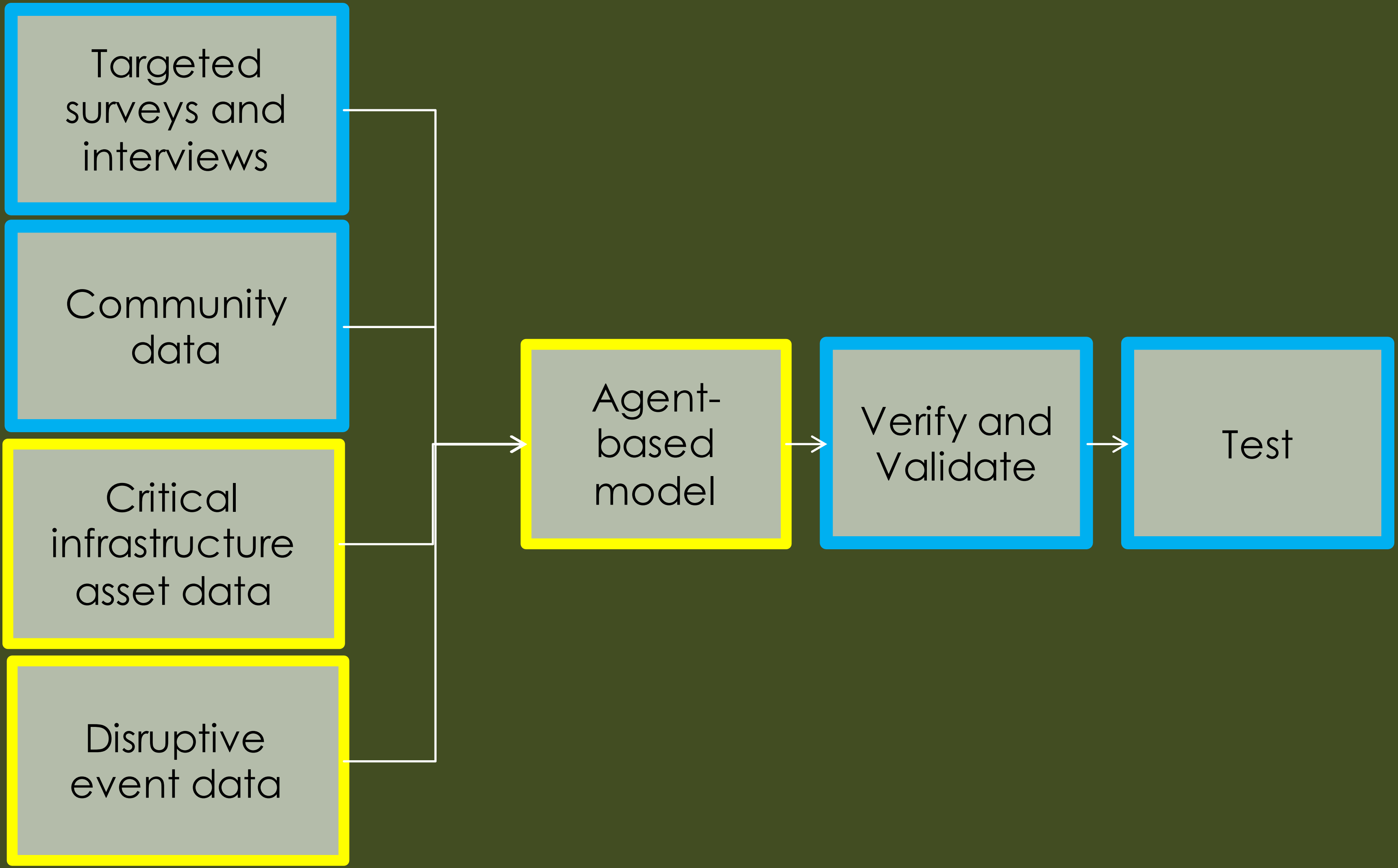
Project Motivation (continued)

- Disruptive events difficult for resource-constrained cities and other jurisdictions
- Resource and capability constraints are relative to both event state and scope
- Volunteer capabilities are important but must be integrated with professional response
- Need to understand interplay between professional and volunteer responders is crucial

Project Goals

- Overall goal
  - Study interdependencies of professional and volunteer responses
    - Response capacities
    - View of community resiliency
    - Resource allocation priorities
    - Relationships between professionals and community
- Methodology
  - Build a proof-of-concept model
  - Validate
  - Test

Current Status and Future Work



Targeted surveys and interviews

Community data

Critical infrastructure asset data

Disruptive event data

Agent-based model

Verify and Validate

Test