Critical Infrastructure Protection (CIP)

John Hoyt
Department of Homeland Security
Science and Technology (S&T) Directorate
john.hoyt@dhs.gov
(202) 401-3467

September 11, 2003

Homeland Security

The Nation's Infrastructure is a Complex "System of Systems"

- **Infrastructure**
  - **The framework of interdependent networks and systems that provides a continual flow of goods and services essential to the defense and economic security of the United States**
- **Critical National Infrastructures**
  - **Infrastructures that are deemed to be so vital that their incapacity or destruction would have a debilitating regional or national impact or would severely disrupt the behavior and activities of large numbers of people who depend upon the infrastructure**

Homeland Security

Critical Infrastructure Protection

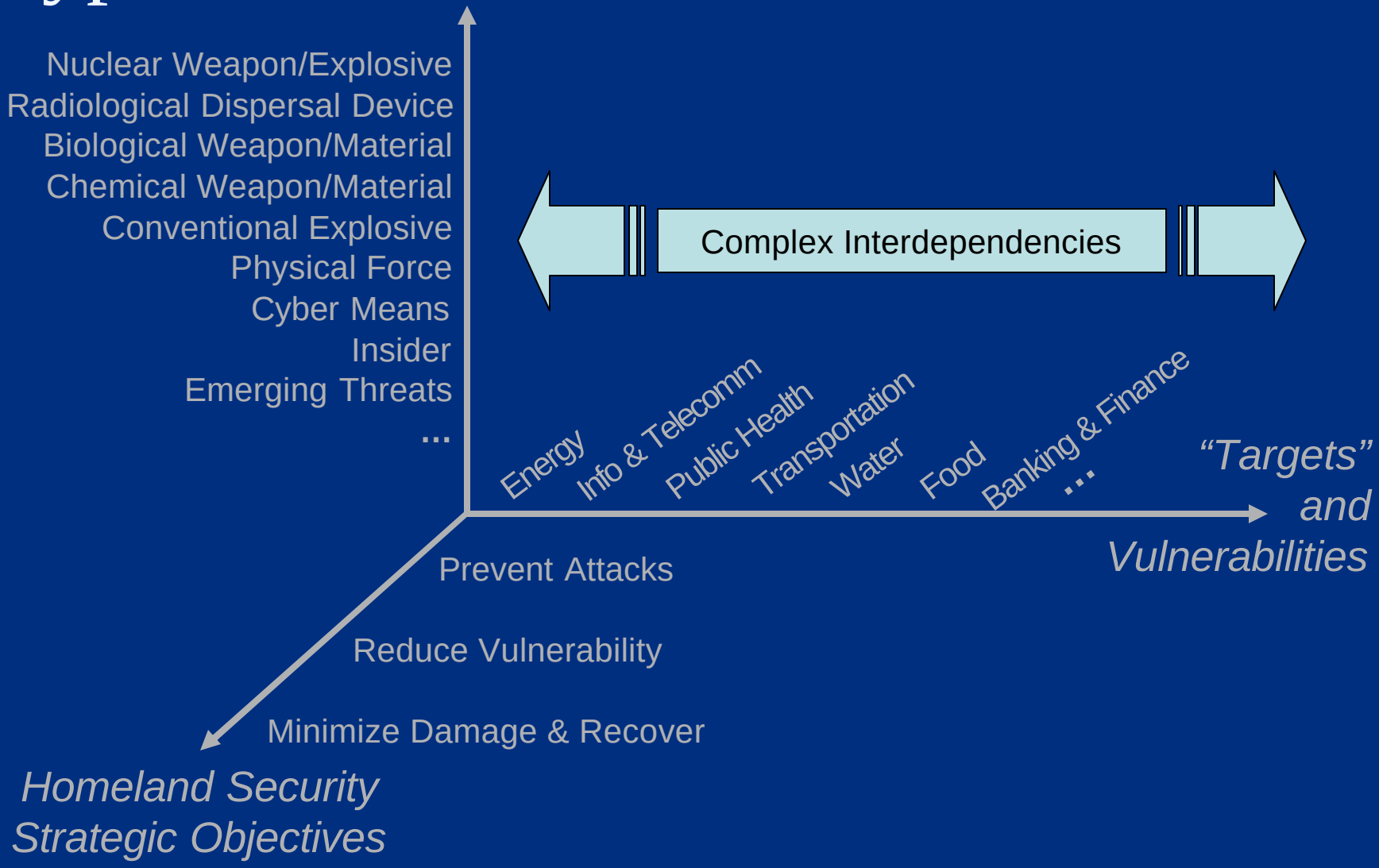
The National Strategy for Homeland Security identifies 14 sectors and key assets that will be protected:

Agriculture	Information & Telecommunications
Food	Energy
Water	Transportation
Public Health	Finance & Banking
Emergency Services	Chemical Industry & Hazardous Materials
Government	Postal & Shipping
Defense Industrial Base	National Monuments & Icons

Most of the Infrastructure is privately owned

Homeland Security

Types of Threats / Means of Attack



Homeland Security

History

- President's Commission on Critical Infrastructure Protection (1997)
- Presidential Decision Directive 63 (1998)
- 1998 CIP R&D Roadmap
- CIP R&D Interagency Working Group
- 2003 National Strategy - cyber security
- 2003 National Strategy - physical security
- Large number of public-private committees and organizations (e.g., Partnership for Critical Infrastructure Security - PCIS)
- Large number of private industry, trade association, and university committees and organizations (e.g., The Infrastructure Security Partnership - TISP)

Future: National S&T Council - Infrastructure Subcommittee, Annual CIP US Government R&D Plan

Homeland Security

CIP R&D Strategy

- Focus on R&D needs appropriate for federal funding (interdependencies, cross cuts, crisis/emergency response)
- Coordinate with other federal and international R&D efforts
- Coordinate with efforts funded by industry
- Build from the 1998 R&D roadmaps and all significant follow-on work (especially post 9/11)
- Invest in areas where there is potential for high payoff and a clear need for high-risk, long-term R&D

CIP R&D Strategy Continued

- Set priorities based on mitigation for highest-risk scenarios and on wide benefit across many infrastructure systems
- Make certain that the “catastrophic” end of the threat spectrum is covered
- Support demonstrations and pilot projects
- Act as an “honest broker” for industry solution systems – certify devices and methods

Key Enabling S&T Areas for CIP

- Analyses, modeling and simulation - for threats, vulnerabilities, consequences, risks, decision support, interdependencies, and complex systems
- Perimeter intrusion detection and warning systems (physical and cyber; detection of “means of attack”)
- Portal scan systems (physical and cyber) for rapid detection of means of attack (CBRNE and cyber)
- Authentication and verification for rapid determination of identity (physical and cyber)

Key Enabling S&T Areas for CIP

- Protection and Mitigation systems
- Portable CBRNE detection systems for emergency responders
- Response and recovery technologies (CBRNE and cyber attacks)
- Information sharing and protection
- Interoperability of communication systems

Risks must be assessed and managed in a dynamic environment

Validate, Verify, Demo, & Test

Red Teams

Generate Scenarios

Decision Support System

- Identification of Critical Nodes
- Consequences of Attacks (cascading effects)
- Measures of Effectiveness
- Investments & Strategies for Prevention, Protection, Mitigation, Response, & Recovery

Homeland Security

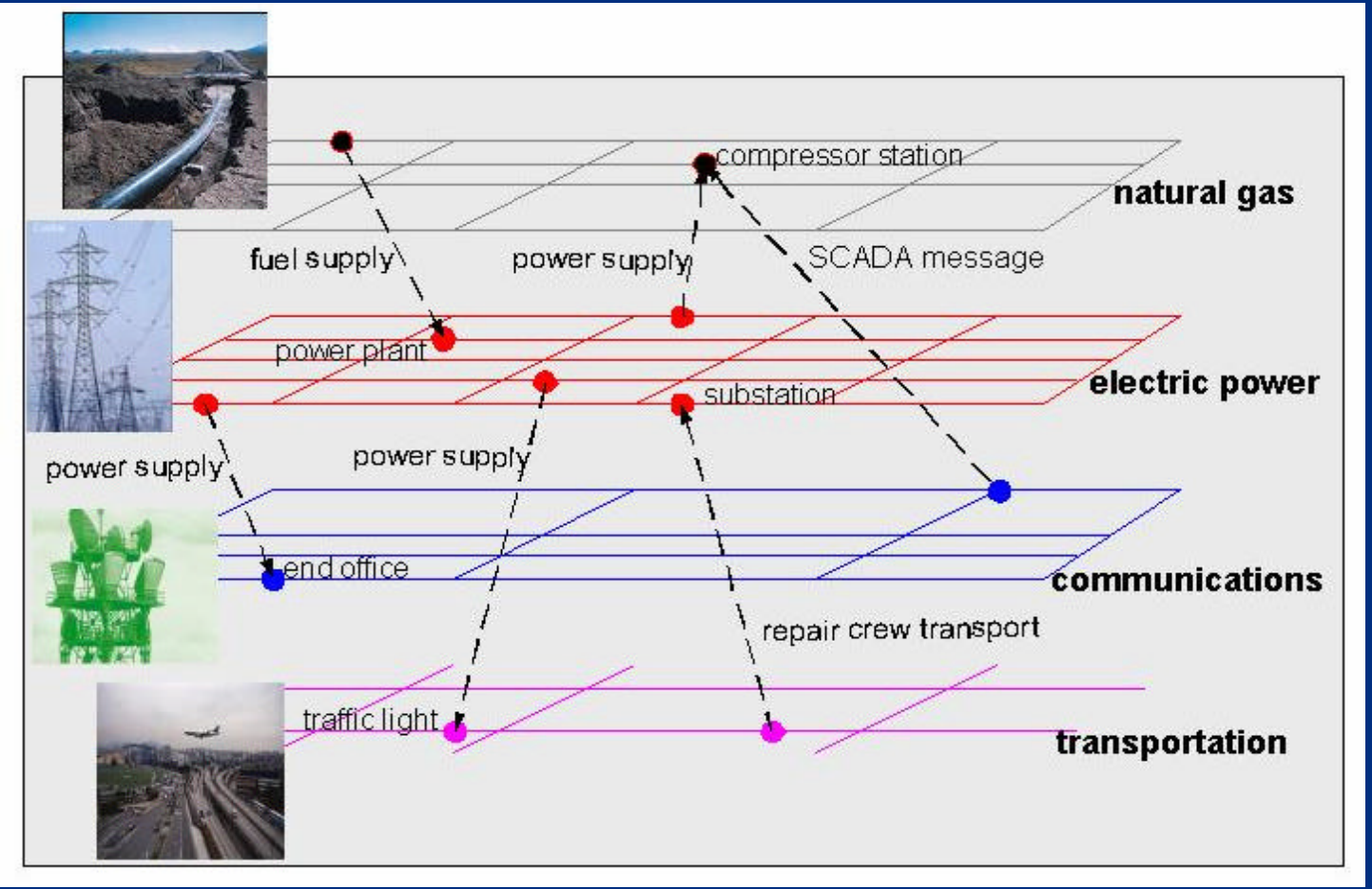
Motivation & Requirements

- Decisions affecting our nation's critical infrastructures are too important to be made without performing analysis beforehand that carefully weighs the benefits of reducing risks with the cost of protective actions.
- Appropriate methodologies can allow decision makers to prioritize and invest scarce resources and to implement rational strategies for protection of various systems and infrastructures based on objective and dynamic modeling, simulation, and analysis.

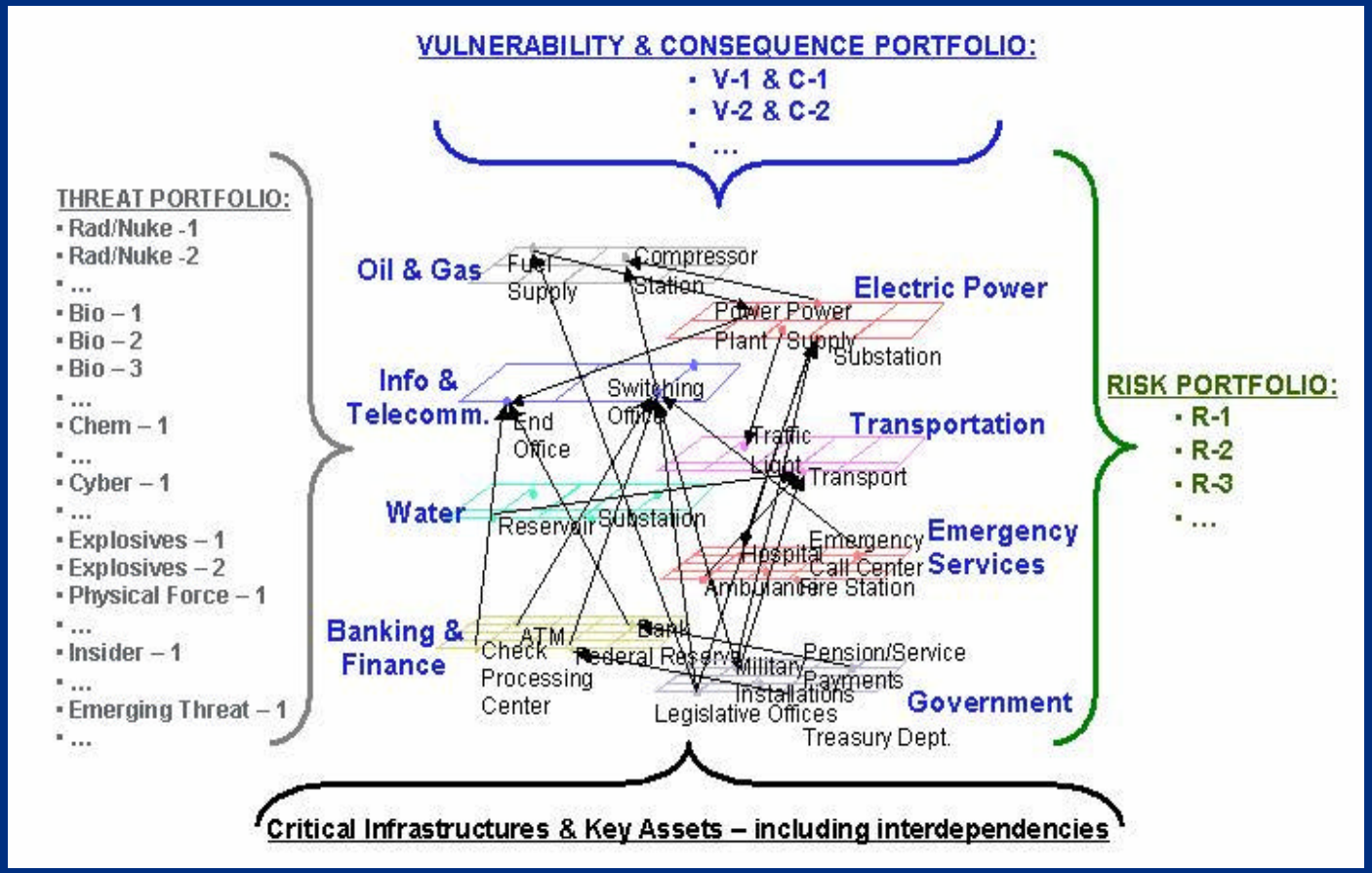
Motivation & Requirements

- In the current and future (dynamic and escalating) threat environment, we need a comprehensive approach to security for our critical infrastructure using vulnerability, consequence, and risk analyses.
  - The approach must address uncertain and evolving threats, consider a wide variety of assets and infrastructures, and use consistent methodologies and criteria.
  - A systems modeling, simulation, and analysis approach can be used to conduct both consequence assessments and risk analyses (based on realistic threats, system/infrastructure vulnerabilities for the threats, and resulting consequences).

Complications: Interdependencies and Organizational Boundaries



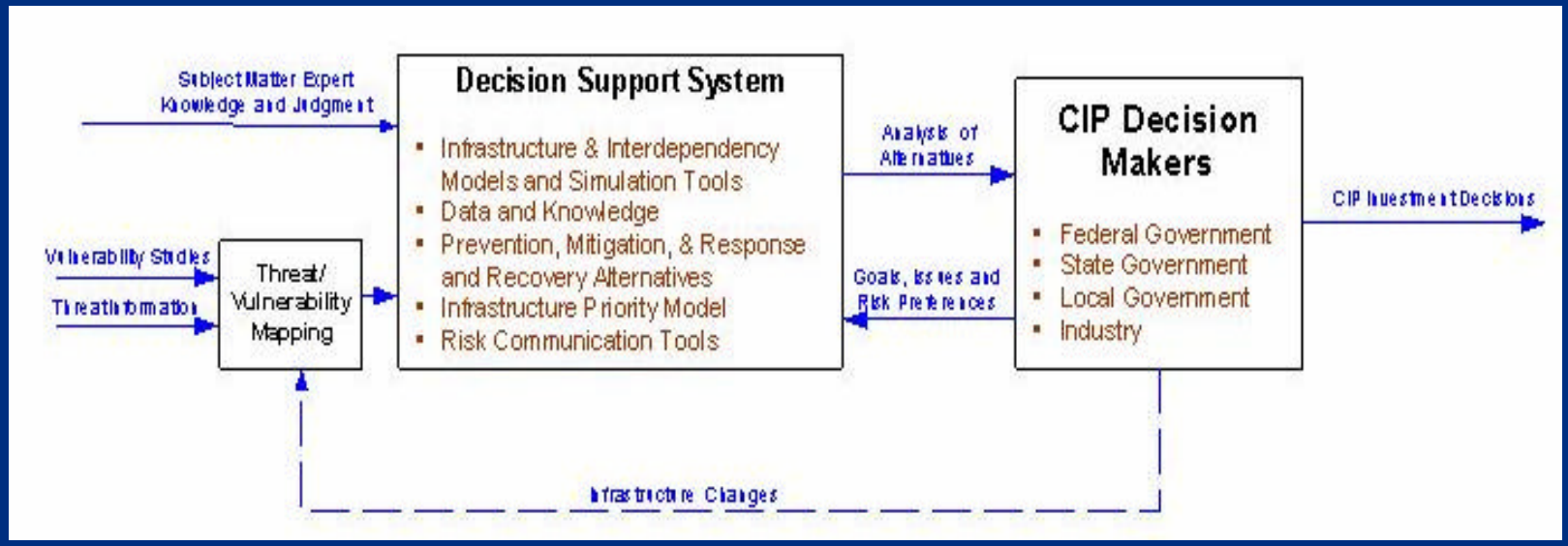
Managing risk for the "system of systems" is an extremely complex undertaking



Homeland Security

Critical Infrastructure Protection Decision Support System

Goal: To develop a Decision Support System that can be used to prioritize protection, mitigation, response, and recovery strategies as well as support red-team and real-time analyses during crises and emergencies.



Approach

Initial focus on consequences

- models of all 14 critical infrastructures and key assets
  - national model prototype
  - metropolitan model prototype
- methodology for analyzing alternatives
- decision support system
  - initial prototype
  - long term architectural plan
- case study preparation

Approach Continued

- Long-term plan
  - iteratively enhance consequence models
  - integrate threat and vulnerability assessments
  - orient decision support system towards unified risk-based evaluations

DHS Cyber Security Program Strategy

- Cyber security" is very large in scope
- Create a cyber security *center* for DHS RDT&E
- The *center* will be the mechanism whereby DHS participates in the cyber security R&D community, and direct its work to address the three- to five-year needs
- Address the priorities identified in the President's *National Strategy to Secure Cyberspace*

DHS Cyber Security Program Strategy

- DHS niche will be to maintain the availability, integrity and confidentiality of the technology that the critical infrastructures rely on
- Focus on mitigating vulnerabilities so that, regardless of the threat and/or actors, the network systems supporting the critical infrastructure of the U.S. remain secure

Why Protect Control Systems?


U.S. DEPARTMENT OF HOMELAND SECURITY
Homeland
Security


Homeland
Security

Cyber Security R&D: Near-Term Goals

- The DHS Cyber Security RDT&E *center* management team will be established and a focus working group convened
- Feasibility study for Secure Border Gateway Protocol (BGP) and Secure Domain Name Services (DNS) to address the scalability and delivery of the protocols to existing systems
- Completion of the Insider Threat behavioral study

Cyber Security R&D: Near-Term Goals

- A feasibility study on technical solutions for patch verification technology to compare patch installation against other hardware and software components on a system
- Co-fund the Cyber Defense Technology Experimental Research Network (DETER Network) – a test bed network for DDoS and Worm research

Mid-Term R&D Efforts in Cyber Security

- Priority access/out-of-band communication – necessity for critical infrastructures to operate through an attack or significant bandwidth consumption
- Techniques and technology for sector assessment – techniques and technology solutions to "grade" sectors on cybersecurity assessments
- Global Internet warning system – address current detection technology problems through standard collector data formats and then address technical solutions for next-generation detection technology

Mid-Term R&D Efforts in Cyber Security

- Insider threat technical solutions – technical solutions based on the findings of the Insider Threat Study
- Intrusion and Misuse Response – tools and techniques for responding to attack or misuse so as to identify, limit and recover from the damage done by an attack and investigate the origin and mechanisms of the attack.

Other Cyber Security Projects of Interest

- Through the technical expertise in the *center*, formulate an on-call response team to support DHS vulnerability remediation needs
- Cooperate with the NSF and NSA in supporting the CyberCorps program
- Technical solutions for secure and reliable software
- Develop statistical data mining methods to find suspicious network traffic and early warning indicators

Homeland Security

BACKGROUND SLIDES

CIAO: CIP Roadmapping Results (July 98)

? Over 70 R&D topics were identified to address infrastructure assurance needs across the eight infrastructures. The following themes describe the focus of these topics:

- **Vulnerability Assessment** —assess the vulnerability of components, systems, and infrastructures.
- **Information Assurance** — secure information while it is stored, being processed, and in transit.
- **Monitoring and Detection** — monitor systems, detect threats and intrusions, and provide timely warning.
- **Protection and Mitigation** — physically protect infrastructures and mitigate damage.
- **Response and Recovery** — aid in rapid incident response and recovery.

CIAO: CIP Roadmapping Results (July 98)

- **Modeling and Simulation** — develop models of components, systems, and infrastructures and examine the efficacy of alternative infrastructure assurance strategies and technologies.
- **Systems Analysis** — analyze complex systems and identify and analyze infrastructure interdependencies.
- **Decision Support** — support timely decision making with tools, methodologies, and information systems.
- **Risk Management** — determine where best to allocate resources and how to manage risks.

- Estimated resource requirements for the R&D topics total approximately $7 billion over the next 10 years.
- Investments beyond those associated with R&D in the critical infrastructures are needed to address interdependency and complexity.

Critical Infrastructure Protection R&D Interagency Working Group (Jan 01)

Eight highest priority R&D issues:

- Establishment of an Institute for Information Infrastructure Protection
- The education and training of research personnel in CIP R&D
- Interdependency analyses
- Threat, vulnerability and risk assessments
- System protection and information assurance
- Reconstitution of damaged or compromised systems
- The security of automated infrastructure control systems
- Intrusion detection and monitoring

National Research Council:

Making the Nation Safer – The Role of S&T in Countering Terrorism (June 02)

Urgent Research Opportunities:

- Develop effective treatments and preventatives for known pathogens for which current responses are unavailable and for potential emerging pathogens.
- Develop, test, and implement an intelligent, adaptive electric-power grid.
- Advance the practical utility of data fusion and data mining for intelligence analysis, and enhance information security against cyberattacks.
- Develop new and better technologies (e.g., protective gear, sensors, communications) for emergency responders.

Homeland Security

National Research Council:

Making the Nation Safer – The Role of S&T in Countering Terrorism (June 02)

Urgent Research Opportunities (continued):

- Advance engineering design technologies and fire-rating standards for blast- and fire-resistant buildings.
- Develop sensor and surveillance systems (for a wide range of targets) that create useful information for emergency officials and decisions makers.
- Develop new methods and standards for filtering air against both chemicals and pathogens as well as better methods and standards for decontamination.

RAND Report (Sept 02) - *Homeland Security: Physical Protection*

Issues and concerns with possible S&T solutions:

- The lack of a single, unified approach to infrastructure protection that integrates physical and cyber elements significantly impedes national planning on homeland security.
- Some critical infrastructure sectors may still fall outside the formal definition and thus receive insufficient priority. The "Human Infrastructure" is being overlooked.
- Information sharing and data protection practices are not up to the task. The public health system is unprepared for its role as critical responder in cases of biological, toxic materials, or radiological attack.

RAND Report (Sept 02) - *Homeland Security: Physical Protection*

Issues and concerns with possible S&T solutions (continued):

- A wide range of infrastructure-specific protective measures face significant problems.
- Control systems and centers may present lucrative targets for attack.
- Operational communication equipment lacks common standards. [There are] Problems in communications interoperability …
- Authentication of identities for personnel … is inadequate.
- Mission-critical personnel need greater protection.
- Critical data on first responders may be stolen and misused.

President's Critical Infrastructure Protection Board:
National Strategy to Secure Cyberspace

National Priorities for R&D:

- Undertake a comprehensive review and gap analysis for outreach, identification, and coordination among R&D providers.
- Define a federal program for R&D on IT security.
- Fund R&D programs of highest priority such as:
  - Intrusion detection
  - Internet infrastructure security
  - Application security
  - Denial of service
  - Communications security including SCADA system encryption/authentication
  - High assurance systems
  - Secure system composition

Homeland Security

President's Critical Infrastructure Protection Board:
National Strategy to Secure Cyberspace

National Priorities for R&D (continued):

- Develop procurement incentives to encourage private sector R&D for highly secure and trustworthy operating systems.
- Examine security implications of emerging technologies.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

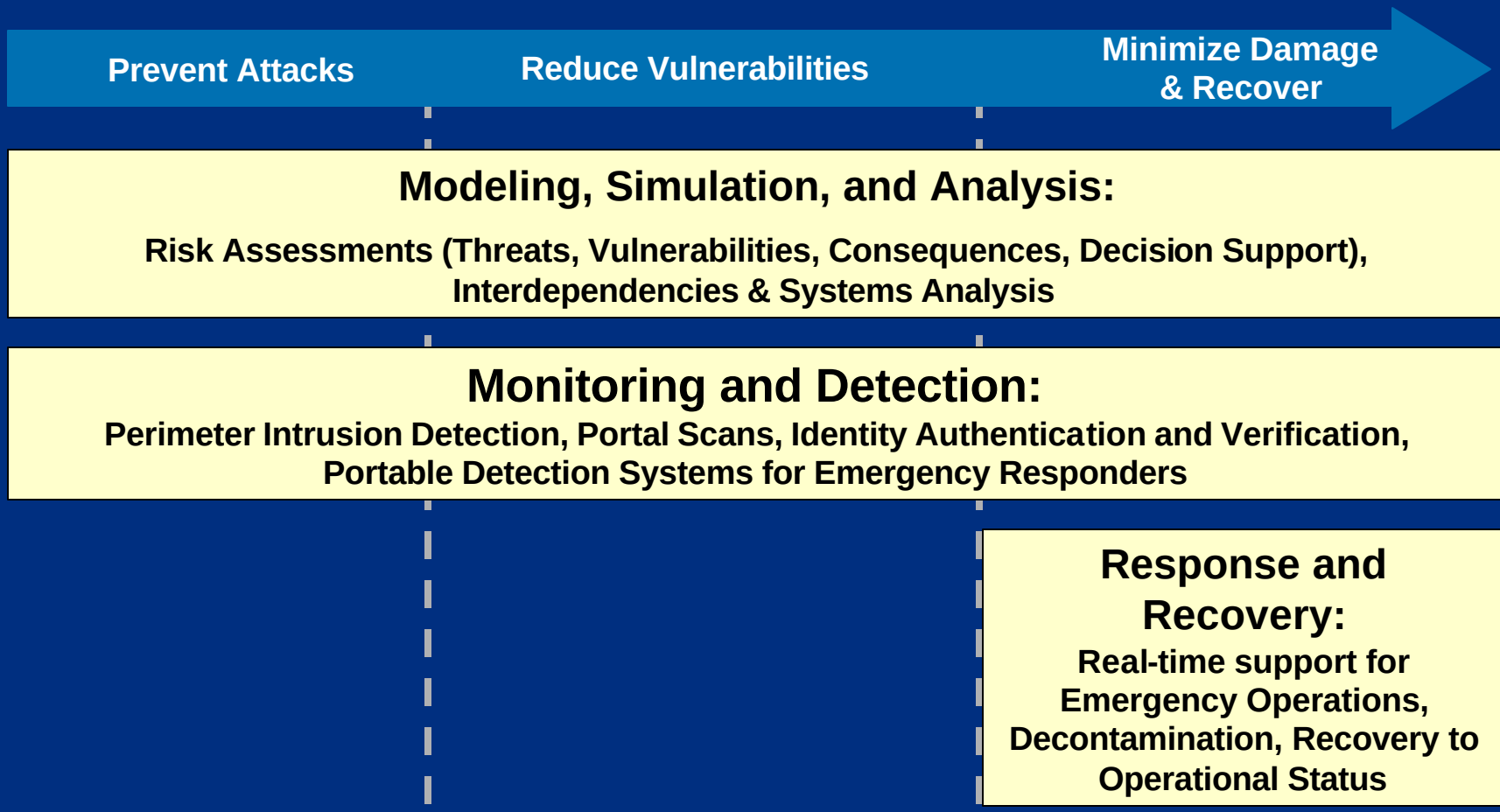
- Coordinate security R&D activities
- Promulgate interoperability standards for communications systems
- Establish method to identify to law enforcement and first responder personnel
- Improve technical surveillance and detection capabilities
- Enable integration of federal analysis/mod/sim into CIP planning and decision-support activities
- Develop economic impact models
- Develop assessment models for physical infrastructure insurance data
- Perform catastrophic disaster analysis

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

(continued)

- Develop node or chokepoint analysis capabilities
- Determine critical interdependencies with system modeling/analysis
- Model sector interdependencies of alerts/warnings procedures/actions
- Initiate work on info “fusion” methods to model interdependencies
- Conduct risk modeling of cyber and physical threats
- Conduct analyses of near simultaneous activation of multiple military operations and plans
- Model optimal distribution/location of sensors in geographically dispersed infrastructures

Critical Infrastructure Protection S&T Roadmap Overview



Modeling, Simulation, and Analysis

- Risk Assessments
  - Threat analysis (provided by the Information Analysis and Infrastructure Protection directorate) – tool development, support, applications
  - Vulnerability analysis (much to be provided by infrastructure owners) – tool development, support, applications
  - Consequence analysis – NISAC and other programs, tool development, support, applications
  - Decision support – NISAC and other programs, tool development, support, and applications

Modeling, Simulation, and Analysis

- Interdependencies and systems analysis (complexity - cascading failures) – NISAC and other programs, tool development and support

Monitoring and Detection

- Perimeter Intrusion Detection (physical & cyber)
  - Physical detection and warning systems
  - Cyber detection and warning systems
  - Intrusion of people, unmanned devices and vehicles, and CBRNE/cyber “means of attack” (e.g., via airborne release)
  - Testing and certification of commercial systems
  - R&D and demonstration of advanced technology
- Portal Scans (physical & cyber)
  - Physical - systems for rapid detection of “means of attack” (CBRNE)
  - Cyber - systems for rapid detection of “attack”
  - Coordinate with CBRNE and cyber efforts
  - Testing and certification of commercial systems
  - R&D and demonstration of advanced technology

Monitoring and Detection

- Identity Authentication and Verification (physical & cyber)
  - Physical - systems to rapidly determine and confirm identity
  - Cyber - systems to rapidly determine and confirm identity
  - Testing and certification of commercial systems
  - R&D and demonstration of advanced technology
- Portable detection systems for Emergency Responders

Response and Recovery

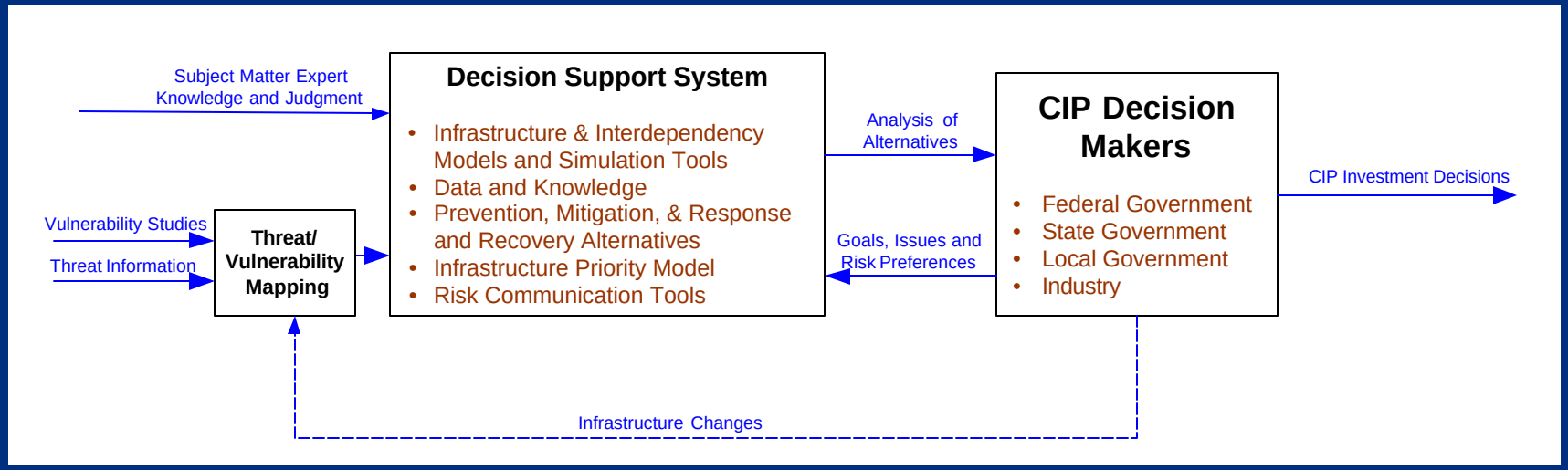
- Real-time support for Emergency Operations
  - Provide analysis of fused real-time incident data
  - Simulate consequences, analyze response and recovery options, and model the impact of allocating available resources

Response and Recovery

- Decontamination and Recovery - technologies to clean-up, rebuild, and return systems to fully operational status (physical & cyber)
  - Coordinate with other efforts:
    - Chemical agent decontamination
    - Biological agent decontamination
    - Radiological decontamination
    - Cyber decontamination and recovery
  - Testing and certification of commercial systems
  - R&D and demonstration of advanced technology

Critical Infrastructure Protection Decision Support System

- Goal: To develop a Decision Support System that can be used to prioritize protection, mitigation, response, and recovery strategies as well as support red-team and real-time analyses during crises and emergencies.



Questions Addressed by CIP Decision Support

- What are the consequences of attacks on our Nation's infrastructure in terms of national security, economic impact, public health, and conduct of government—including the consequences that propagate into one or more infrastructures?
- Are there choke points in our Nation's infrastructures (i.e., those areas where one or two attacks could have the largest impact)? What/where are the choke points?
- Incorporating consequence, vulnerability, and threat information into an overall risk assessment, what are the highest risk areas?
- What investment strategies can the U.S. make that will have the most impact in reducing overall risk?

Homeland Security

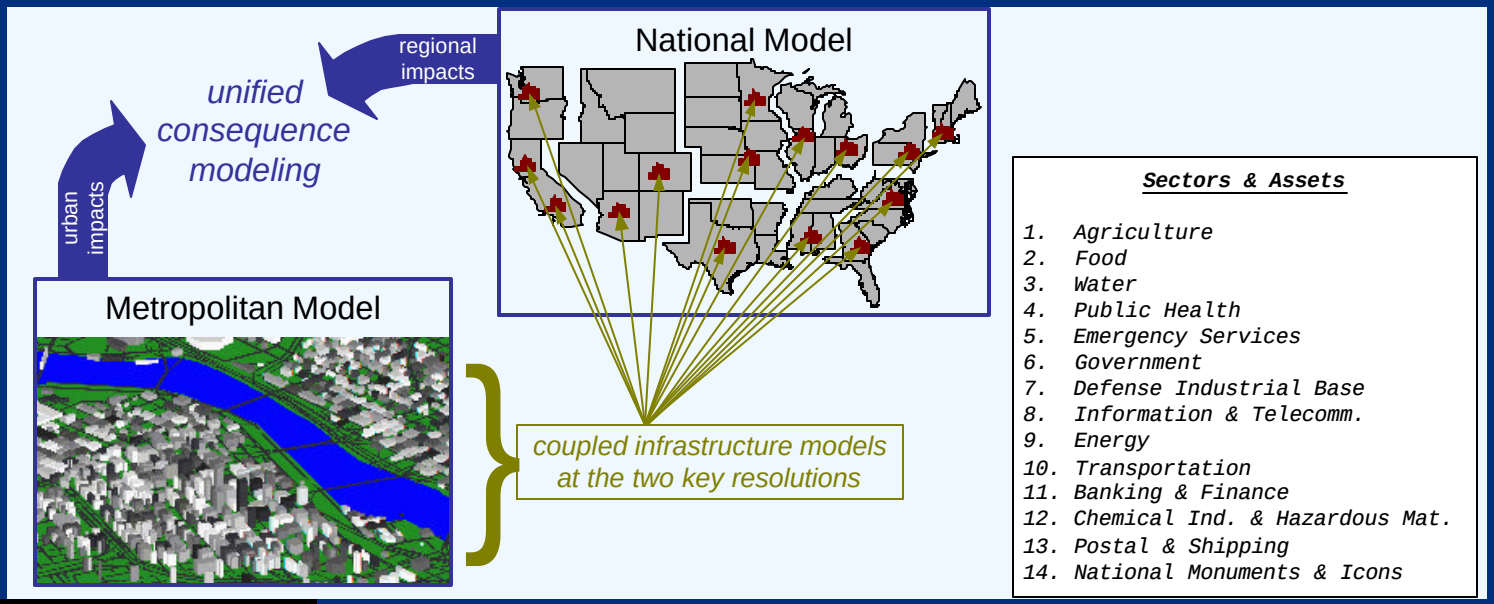
Relevance to the Department of Homeland Security Mission

- The long-term CIP/DSS program plan partially or fully addresses all of the modeling, simulation, and analysis (MS&A) elements of the "National Strategy for the Physical Protection of Critical Infrastructure and Key Assets":
  - Enable the integration of modeling, simulation, and analysis into . . . protection planning and decision support activities
  - Develop economic models of near- and long-term effects . . .
  - Develop critical node/chokepoint and interdependency analysis capabilities;
  - Model interdependencies across sectors . . .
  - Conduct integrated risk modeling . . .
  - Develop models to improve information integration

Homeland Security

Task 1. Develop Unified Critical Infrastructure Models

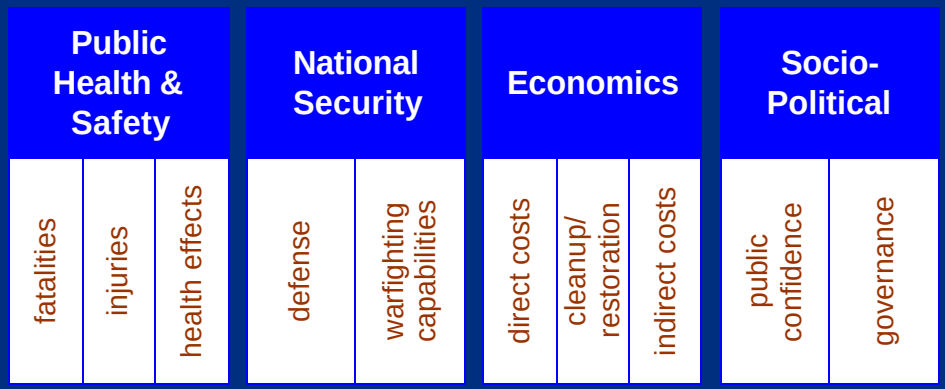
- Most infrastructures have both national and metropolitan aspects.
  - e.g., interstate transport of water vs. municipal water delivery
- We aim to develop integrated models of all 14 sectors/assets at both geographic scales, and their interdependencies.
- Work will proceed iteratively, where models are refined sequentially to provide better consequence estimates and more thorough treatment of interdependencies.



Homeland Security

Task 2. Develop Methodology for Analysis of Alternatives

- Goal: To measure impacts of infrastructure disruptions.
- Approach:
  - A broad range of metrics will be defined.
  - Metrics will be calculated from the output of the national and metropolitan consequence models.
  - Direct & secondary effects of disruptions and side benefits of policy will be quantified.
  - Impacts will be presented in an accessible and transparent form for decision makers.
- Products:
  - consequence measurement hierarchy
  - metric calculation techniques
  - prioritization methodology



Task 3. Design and Development of DSS Architecture

- We take an iterative approach to developing and refining a unified decision support capability for critical infrastructure protection.
- Our near-term efforts aim to provide an initial prototype supporting the immediate needs of decision makers.
  - The short time frame for an initial operational capability precludes full architectural development.
  - An initial prototype will elucidate many of the major issues that must be addressed in the long term.

Task 3. Design and Development of DSS Architecture

- Our long-term efforts will result in a robust, unified architecture for CIP decision support.
  - The treatments of consequence, threat, vulnerability, risk, uncertainty, and metrics all must cooperate seamlessly to ensure the usability of the CIP/DSS.
  - The risks to the success of this project are minimize by tackling major issues sequentially.

Task 4. Apply CIP/DSS Prototype to a Case Study

- Goal: To demonstrate to CIP decision makers how our decision support system would be applied in making real world decisions.
- Approach:
  - We will plan a specific case study application for the CIP/DSS.
  - We will identify a selected set of CIP decision makers at the metropolitan, regional, state, and national level to participate in the studies.
  - We will use their experience in framing the main features and elements of the case study.
- Products:
  - status report for case study plan