

---

*Research and  
Development for  
Critical  
Infrastructure  
Protection*



**John Davis  
Commissioner**

---



# R&D Issue for Critical Infrastructure Protection

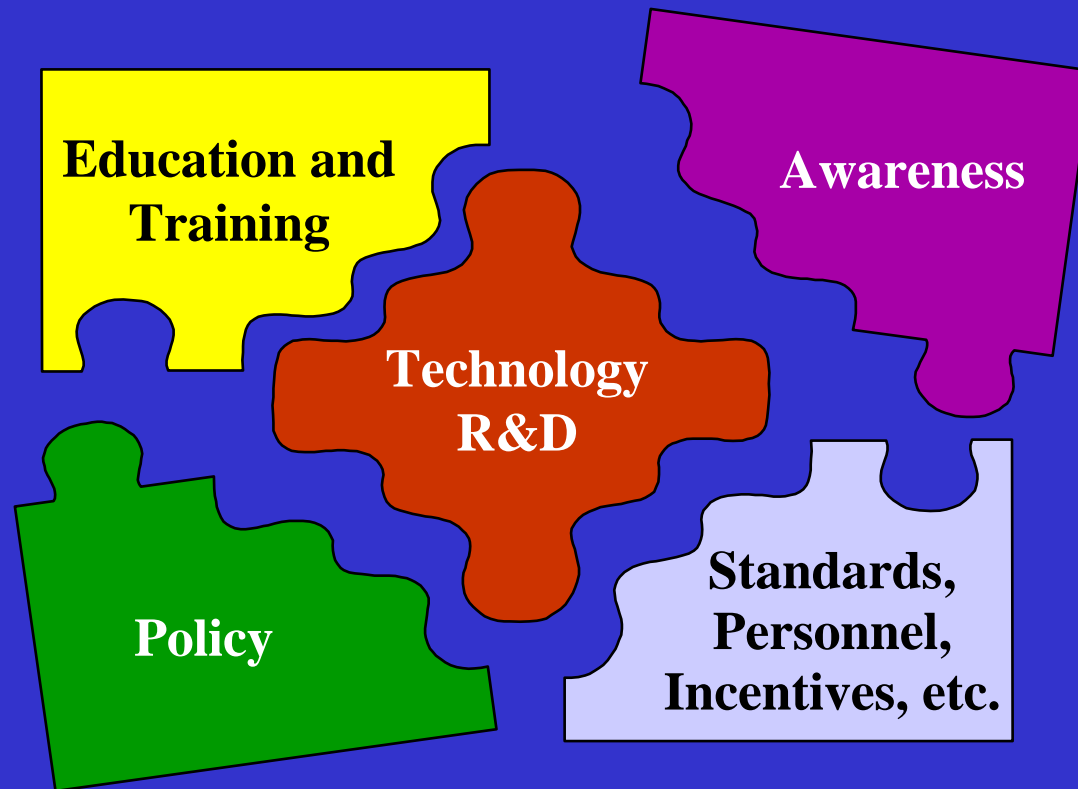
- ◆ What should be done?
- ◆ What investment is needed?
- ◆ Who should do it?

*What is the proper balance between  
the public and private sector for  
R&D investment?*

# The Goal of R&D Is to Develop Technologies that Would Meet Assurance Objectives



# R&D Is Only One Piece of the Overall Infrastructure Assurance Puzzle





# Observations

- ◆ New technologies are needed to effectively deal with the current and future vulnerabilities
- ◆ Research is sponsored by multiple agencies of the government
- ◆ Annual funding range for information assurance R&D is \$150M (government): \$120M - 355M (industry)
- ◆ Research investment is inadequate, and progress is too slow



# Observations (*cont'd*)

- ◆ Private sector will not invest significant resources in long-term research for sound business reasons
- ◆ Private sector develops technology (i.e., the tools, techniques, methods, and equipment used in building the various infrastructures)
- ◆ Private sector develops technology for in-house application & perceived markets
- ◆ Next Generation Internet (NGI) provides an opportunity to rebuild the Internet with high assurance

# Process for Developing Integrated R&D Recommendations

## **NSA Study:**

INFOSEC research in the DoD and Intelligence Community



## **NRC Interim Report:**

Information Systems Trustworthiness



## **DARPA**

Information Survivability



**NAS, DSB, DoD, and other Studies**



**Integrated R&D Recommendations**

## **DOE National Lab R&D Studies; Surveys and Interviews**

- ◆ Information and Communications
- ◆ Electric Power
- ◆ Oil & Gas Transportation & Storage
- ◆ Transportation
- ◆ Banking & Finance
- ◆ Water
- ◆ Emergency Services
- ◆ Government Services
- ◆ Crosscutting/Interdependencies

**Bellcore**  
R&D for Network Assurance in 2010

**IDA Study:**  
Private sector research in information assurance

**Stakeholder Input (e.g. Council on Competitiveness)**

# Electric Power System R&D Study

## R&D Team:

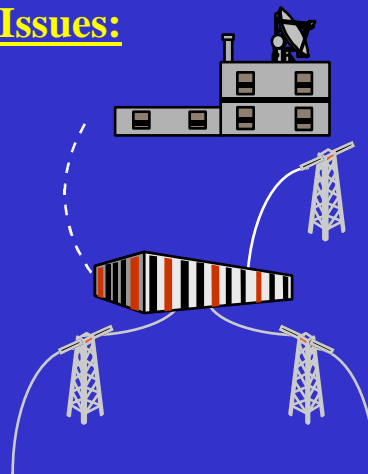
- ◆ Argonne National Lab (lead)
- ◆ Brookhaven National Lab
- ◆ Lawrence Berkeley National Lab
- ◆ Los Alamos National Lab
- ◆ Oak Ridge National Lab
- ◆ Pacific Northwest National Lab
- ◆ Sandia National Lab

## Stakeholders Contacted:

- ◆ Bonneville Power Administration (BPA)
- ◆ Commonwealth Edison
- ◆ Edison Electric Institute (EEI)
- ◆ Electric Power Research institute (EPRI)
- ◆ North American Electric Reliability Council (NERC)
- ◆ Wisconsin Public Service Commission
- ◆ Others

## Threat and Vulnerability Issues:

- ◆ Restructuring
- ◆ Transmission system reliability
- ◆ Physical threats to transmission facilities
- ◆ Cyber threats to SCADA systems
- ◆ Disgruntled employees



## R&D Program Topics:

- ◆ On-line security assessment
- ◆ Real-time control mechanisms
- ◆ Transmission and distribution technology
- ◆ Evaluation of current and future electric power systems
- ◆ Information security

# Water Supply R&D Study

## R&D Team:

- ◆ Argonne National Lab
- ◆ Oak Ridge National Lab
- ◆ Pacific Northwest National Lab (lead)

## Stakeholders Contacted:

- ◆ City and state government offices
  - departments of public works
  - environmental protection
  - emergency management/response
- ◆ Environmental Protection Agency
- ◆ Bureau of Reclamation
- ◆ National Center for Public Health
- ◆ Others

## Threat and Vulnerability Issues:

- ◆ Chemical threats
- ◆ Biological threats
- ◆ Physical
- ◆ Natural hazards
- ◆ Cyber
- ◆ Aging infrastructure



## R&D Program Topics:

- ◆ Automated detection and analysis
- ◆ Integrated system status monitoring technology
- ◆ Remote sensing and GIS
- ◆ Improved methods of water purification
- ◆ Protocols for on-line SCADA systems

# Process for Developing Integrated R&D Recommendations

## NSA Study:

INFOSEC research in the DoD and Intelligence Community

## NRC Interim Report:

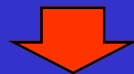
Information Systems Trustworthiness

## DARPA

Information Survivability

## NAS, DSB, DoD,

and other Studies



**Integrated R&D Recommendations**



## DOE National Lab R&D Studies; Surveys and Interviews

- ◆ Information and Communications
- ◆ Electric Power
- ◆ Oil & Gas Transportation & Storage
- ◆ Transportation
- ◆ Banking & Finance
- ◆ Water
- ◆ Emergency Services
- ◆ Government Services
- ◆ Crosscutting/Interdependencies


**Bellcore**  
R&D for Network Assurance in 2010

**IDA Study:**  
Private sector research in information assurance

**Stakeholder Input (e.g. Council on Competitiveness)**



# Information Security Research and Technology



# INFOSEC Research and Technology Program

- ◆ INFOSEC Research Council
  - <http://doe-is.llnl.gov>
- ◆ INFOSEC Science and Technology Study Group
- ◆ Academic capability development
- ◆ University research program

Technical Workshops  
National Technical Baseline for INFOSEC  
Technology Forecasting

Civilian Universities  
DoD Universities  
Faculty, Staff, Students

**U.S. Government Sponsors  
INFOSEC Research Council**

NIST    DARPA    DISA    NSA

MILITARY SERVICES    DOE    CIA

National Security Needs  
Warfighter needs

Industry and Academia  
INFOSEC  
Science & Technology  
Study Group  
Leading Experts

Research Institutes  
FFRDCS & Industry  
Research Staff Members

Security Solutions  
Security Solutions



# Information Systems Trustworthiness

Interim Briefing: April 16, 1997

Stephen D. Crocker & Fred B. Schneider  
Co-chairs

Majory S. Blumenthal, Director

Computer Science and  
Telecommunications Board



# Trustworthiness is . . .

- ◆ A set of attributes to justify dependence:
- ◆ Users must get “right” outputs, unaffected by environmental realities including:
  - Hardware failures
  - Acts of malice by users and intruders
- ◆ A holistic property:
  - Property of a system, not only of components.
  - Involves many interacting sub-properties.



# Evolving a National Information Assurance Research Agenda:

## Evolving a National Information Assurance Research Agenda: Issues and Opinions From Commercial Information Technology Providers

William T. Mayfield  
Ron S. Ross



# 21 Technology Providers Interviewed

## Large Companies

- ◆ IBM
- ◆ Hewlett-Packard
- ◆ Sun Microsystems
- ◆ Novell
- ◆ 3COM
- ◆ CISCO
- ◆ Lucent Technologies
- ◆ AT&T
- ◆ Intel
- ◆ Motorola
- ◆ Oracle
- ◆ Sybase
- ◆ Microsoft

## Niche Companies

- ◆ Gemini Computing
- ◆ Secure Computing Corp.
- ◆ Trusted Information Systems
- ◆ Raptor
- ◆ Security Dynamics
- ◆ Spyrus
- ◆ Haystack Computing
- ◆ WheelGroup



# IDA Study Findings

- ◆ *Finding 1.* The information needed to definitively quantify commercial IA research funding was not available.
- ◆ *Finding 2.* All the companies interviewed indicated that their R&D investments in IA technology were increasing and that for most companies, this trend should continue for the next few years.
- ◆ *Finding 3.* A gross estimate of commercial IA R&D funding ranges between \$120 million to \$355 million per year.
- ◆ *Finding 4.* The U.S. commercial IA R&D activity is fairly robust.



# Bellcore Key Recommendations on R&D

The key recommendations of this study are that the government should maintain at least its current level of R&D funding and take steps to promote R&D in critical areas that directly impact network assurance

- ◆ Security (OS security, software integrity, cryptography, intrusion detection, and firewalls)
- ◆ Distributed control (middleware - OAM, services) Network assurance measurement infrastructure (metrics, criteria, techniques, and tools)
- ◆ Interprovider policy routing/architecture
- ◆ Advance services (QoS, multicast)
- ◆ Stability of dynamic IP and ATM routing protocols
- ◆ New technologies, services, and applications



# Research Is Needed to:

- ◆ Secure information while stored, in transit, and in process
- ◆ Monitor and detect active threats, and notify in real time
- ◆ Assess vulnerability of both elements and entire infrastructures
- ◆ Manage risk and support decision making
- ◆ Protect infrastructures physically and mitigate damage
- ◆ Plan for contingencies and emergency response and recovery



# R&D Needs Were Grouped into Six Topical Categories

- ◆ Information assurance
- ◆ Monitoring and threat detection
- ◆ Vulnerability assessment and systems analysis
- ◆ Risk management and decision support
- ◆ Protection and mitigation
- ◆ Contingency planning, incident response, and recovery



# Information Assurance is a Key Component to the Functioning of Our Interdependent Infrastructures

## ◆ Objectives

- Protect communications infrastructure
- Protect information while stored, processed, and transmitted

## ◆ Specific R&D needs

- Security architectures
- Advanced concepts and theory
- Management of information protection
- Encryption technologies
- System characterization
- Human/social



# Monitoring and Threat Detection Would Provide Early Threat Warning

## ◆ Objectives

- Identify attacks with reliable, automated monitoring and detection technologies
- Characterize attacks using data reduction and analysis tools

## ◆ Specific R&D needs

- Automated monitoring and detection
- Intelligence/information collection
- Data reduction and analysis
- Infrastructure information system



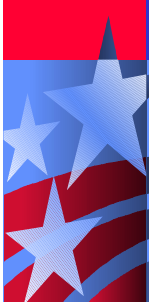
# Vulnerability Assessment & Systems Analysis Tools Identify Weaknesses in Systems & Components

## ◆ Objectives

- Identify critical nodes, examine interdependencies, and understand complex systems
- Address physical and cyber security issues in an integrated mode

## ◆ Specific R&D needs

- Vulnerability assessment tools
- Infrastructure and nodal analysis tools
- Complex system modeling
- Test beds
- Verification technologies



# Risk Management and Decision Support Tools Aid in the Allocation of Limited Resources and Reduce Risk

## ◆ Objectives

- Evaluate risks from historical, current, and future threats
- Support real-time decision making

## ◆ Specific R&D needs

- Risk management tools
- Consequence modeling and analysis
- Decision analysis
- Real-time predictive models
- Lessons learned systems



# Protection and Mitigation Measures Protect Infrastructures From a Wide Spectrum of Threats

## ◆ Objectives

- Protect and improve the effectiveness of existing infrastructures
- Mitigate potentially large disruptions

## ◆ Specific R&D needs

- Real-time system control
- Infrastructure hardening
- Isolation & containment technologies



# Contingency Planning, Incident Response, & Recovery Technologies Are Needed to Minimize Impacts

## ◆ Objectives

- Support effective crisis and consequence management
- Aid in rapid recovery and restoration of services

## ◆ Specific R&D needs

- Contingency, response, and recovery planning tools
- Response technologies (e.g, to support emergency responders)
- Recovery technologies (e.g., decontamination, information recovery technologies)



# Increased R&D Is Needed Now

- ◆ *R – Research* – sponsored mostly by the government; long term, new concepts, national scale
- ◆ *D – Development* – sponsored mostly by industry; tools, techniques, methods, and equipment created and offered for sale by the private sector, and installed to upgrade existing infrastructures



# A Joint R&D Effort Involving Government, Industry, & Academia Should Be Established

- ◆ Risks cut across the public and private sectors
- ◆ Much of the relevant technical and empirical data on infrastructure operations, interdependencies, and vulnerabilities are held by the private sector
- ◆ Training, education, and awareness programs are needed to develop a cadre of knowledgeable people (“infrastructure assurance practitioners”)
- ◆ Successful implementation will require closer cooperation between government, academia, and the private sector



# Recommendations

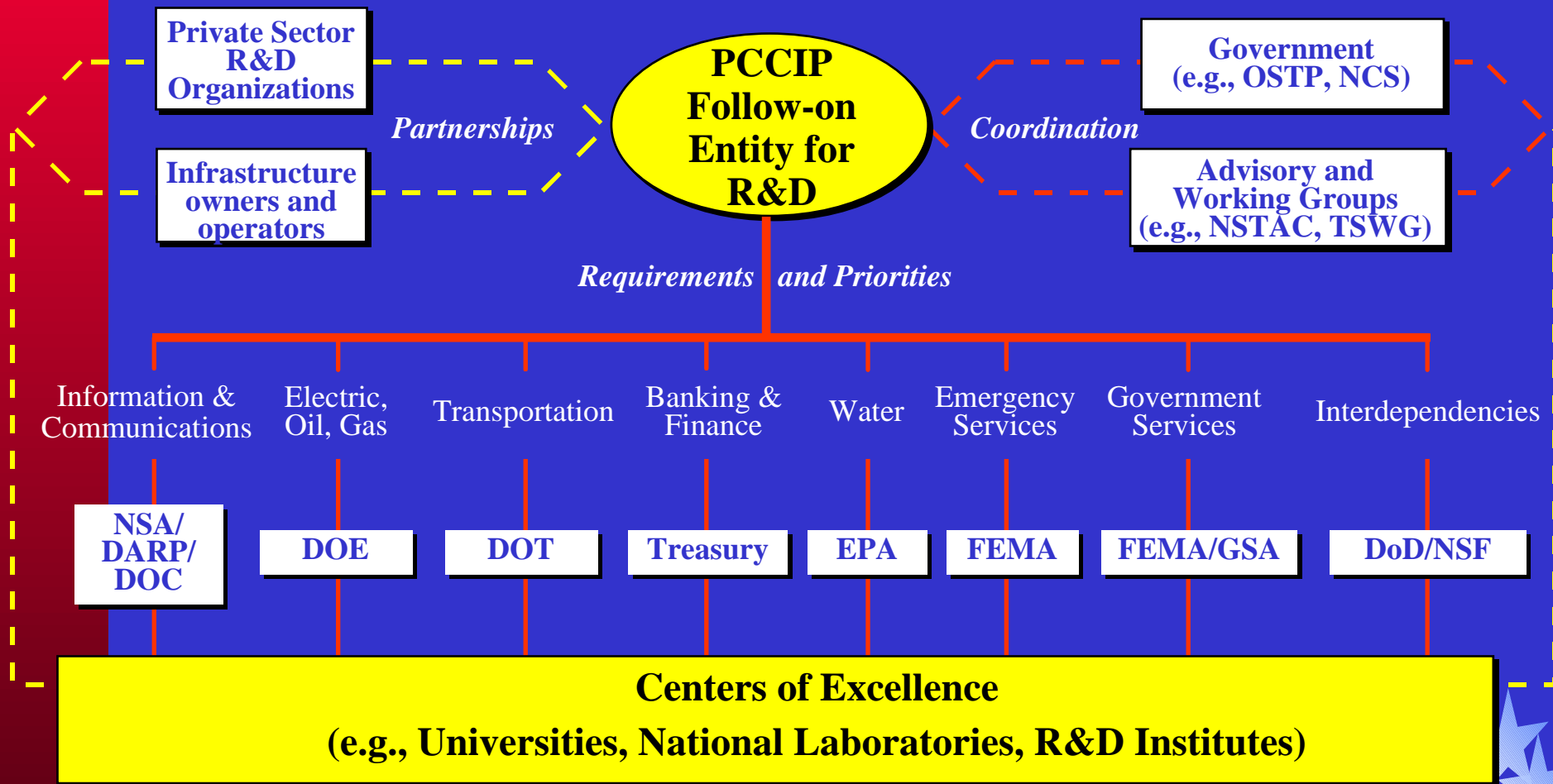
- ◆ Conduct a detailed analysis of infrastructure R&D needs and priorities prior to establishing a final National R&D Program for Infrastructure Assurance
- ◆ Designate appropriate government departments and agencies to manage infrastructure-specific R&D efforts
- ◆ Promote the “science” of complex, interdependent systems and conduct in-depth research that addresses national infrastructure issues



# Recommendations (*cont'd*)

- ◆ Establish a national repository of validated infrastructure-related models & data (e.g., test beds)
- ◆ Create forums that bring together researchers, infrastructure owners and operators, & government to discuss common problems, requirements, & solutions
- ◆ Promote education, training, & certification programs to ensure proper implementation & utilization of new technologies, methods, & tools

# R&D Structure



# Recommended Government Infrastructure Assurance R&D Investments

R&D Investment Category	<i>Investment (\$ Millions)</i>						
	FY98	FY99	FY00	FY01	FY02	FY03	FY04
Information Assurance	150	300	360	420	480	540	600
Other Areas of Infrastructure Assurance	100	200	240	280	320	360	400
<b>Total</b>	<b>250</b>	<b>500</b>	<b>600</b>	<b>700</b>	<b>800</b>	<b>900</b>	<b>1,000</b>

**National Research Council study to validate or adjust investment**



# R&D Issue for Critical Infrastructure Protection

- ◆ What should be done?
- ◆ What investment is needed?
- ◆ Who should do it?

*What is the proper balance between  
the public and private sector for  
R&D investment?*