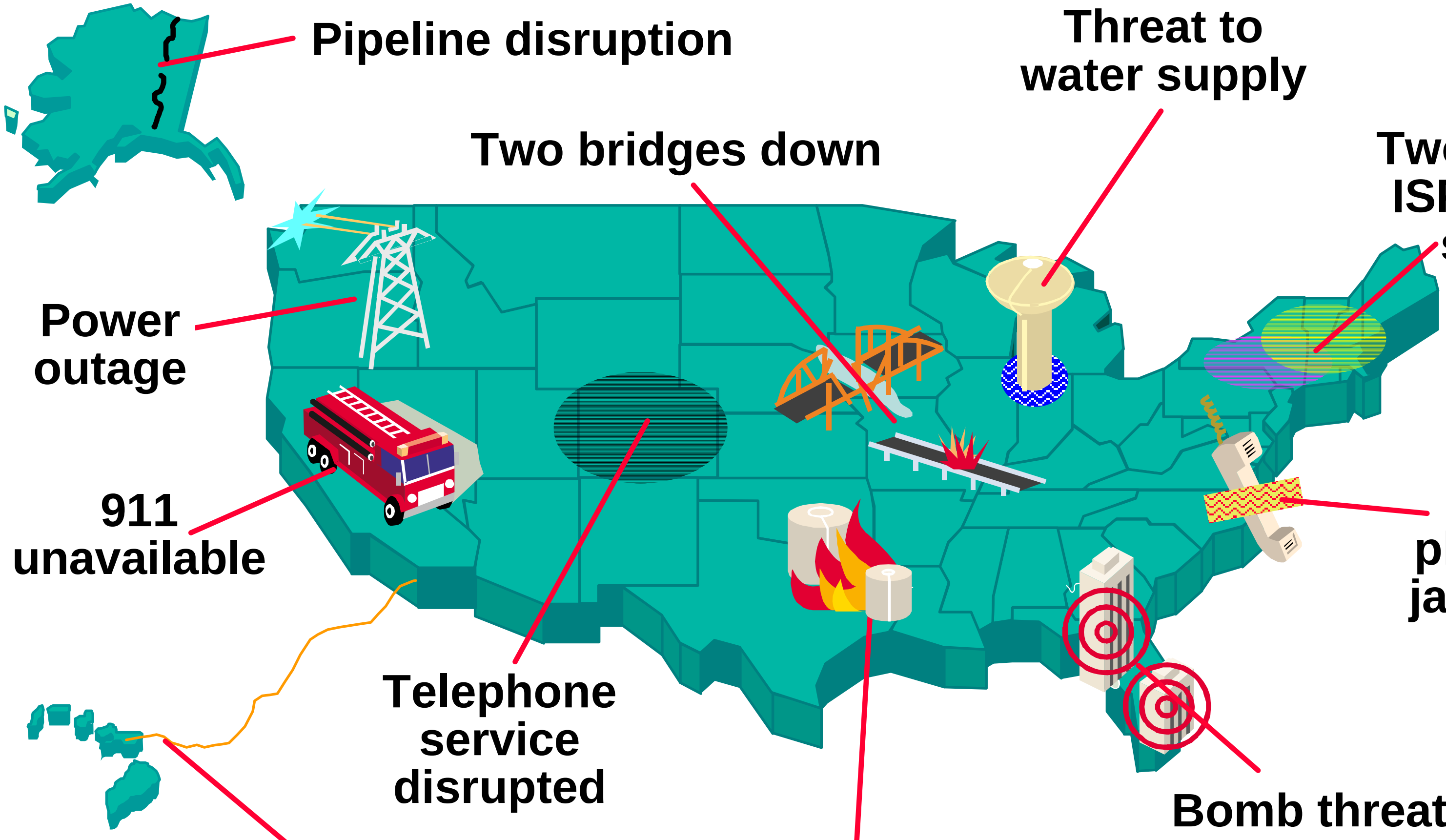
President’s Commission on
Critical Infrastructure Protection

Critical Foundations

Protecting America’s Infrastructures

1997

Imagine ...



Pipeline disruption

Threat to water supply

Two bridges down

Two regional ISP's out of service

Power outage

911 unavailable

FBI phones jammed

Telephone service disrupted

Submarine cable lost

Oil refinery fire

Bomb threats in two buildings

What Do We Do?

- Whom do you call?
- What do you need to know?
- How quickly?
- Why?
- Is it coincidence?
- Can you respond?

Progress Report

- ♦ **The Commission**
- ♦ Vulnerabilities and Threats
- ♦ Findings
- ♦ Recommendations

Mission

Recommend a national policy
for protecting and assuring
critical national infrastructures

- ♦ Determine vulnerabilities
- ♦ Identify threats—physical, cyber
- ♦ Develop policy & legislative issues
- ♦ Develop policy recommendations & implementation plan

Critical Infrastructures

- ♦ Telecommunications
- ♦ Electric Power
- ♦ Transportation
- ♦ Oil & Gas
  Delivery & Storage
- ♦ Banking & Finance
- ♦ Water
- ♦ Emergency Services
- ♦ Government Services

Why Attack Infrastructures?

National Security

Reduce US ability to act in its own self interest

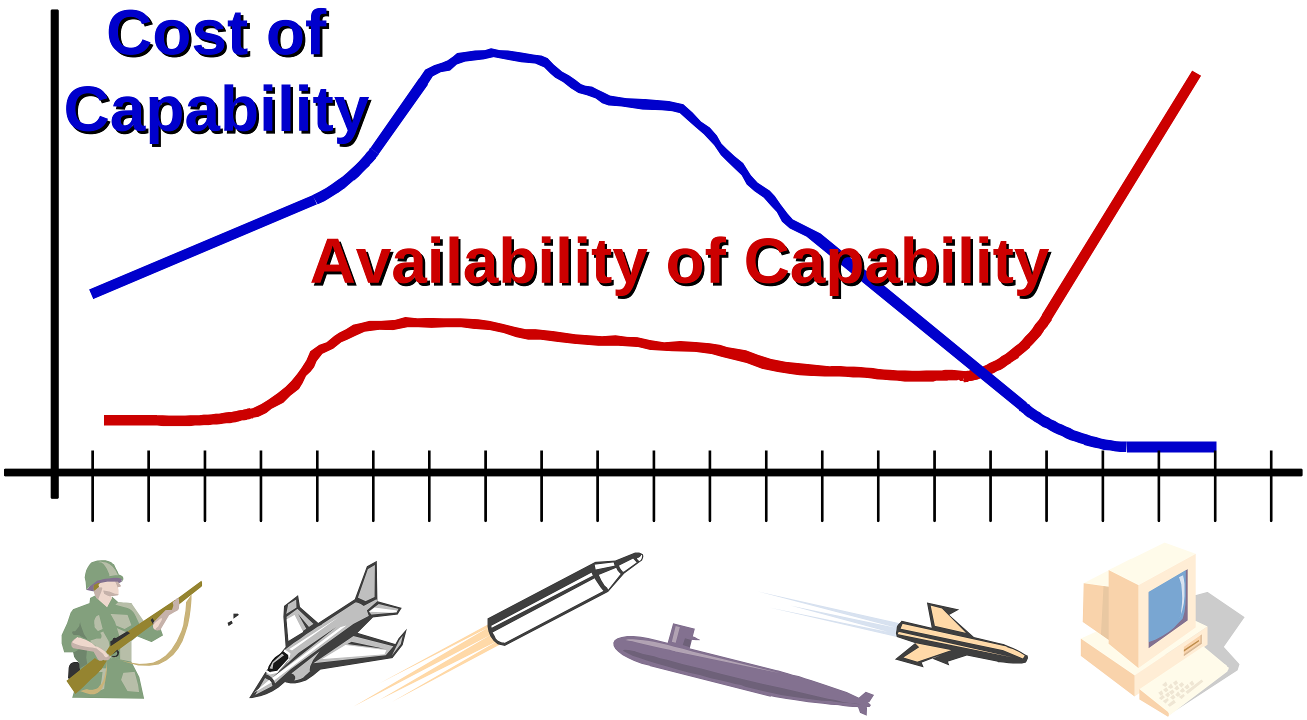
Public Welfare

Erode confidence in critical services

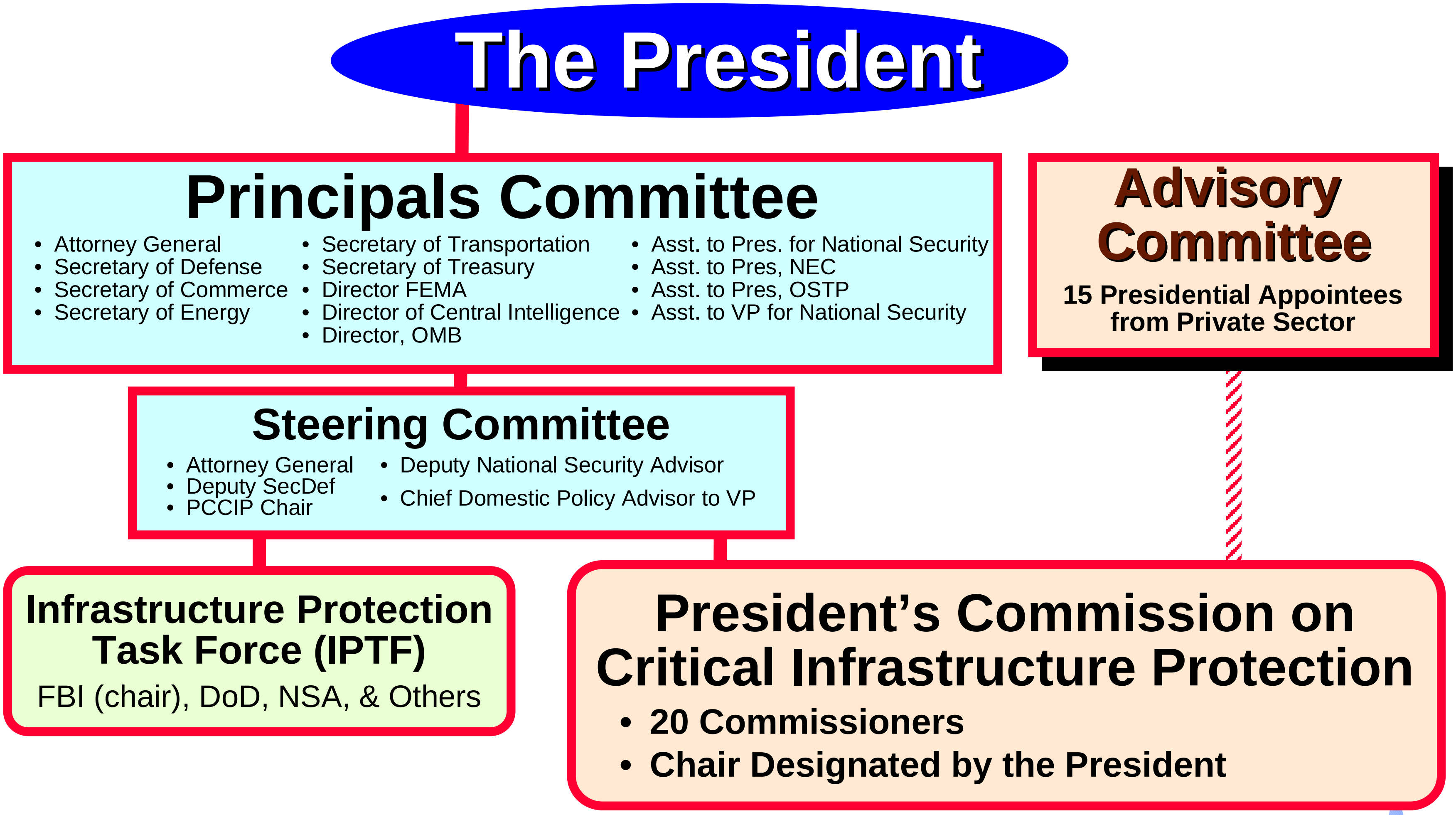
Economic Strength

Damage American economic competitiveness

Evolution of Threat



The Structure



The President

Principals Committee

- Attorney General
- Secretary of Defense
- Secretary of Commerce
- Secretary of Energy
- Secretary of Transportation
- Secretary of Treasury
- Director FEMA
- Director of Central Intelligence
- Director, OMB
- Asst. to Pres. for National Security
- Asst. to Pres, NEC
- Asst. to Pres, OSTP
- Asst. to VP for National Security

Advisory Committee

15 Presidential Appointees from Private Sector

Steering Committee

- Attorney General
- Deputy SecDef
- PCCIP Chair
- Deputy National Security Advisor
- Chief Domestic Policy Advisor to VP

Infrastructure Protection Task Force (IPTF)

FBI (chair), DoD, NSA, & Others

President's Commission on Critical Infrastructure Protection

- **20 Commissioners**
- **Chair Designated by the President**

Commissioners

Public Sector

CIA

FBI

FEMA

NSA

Department of Commerce

Department of Defense

Department of Energy

Department of Justice

Department of Transportation

Department of Treasury

Private Sector

AT&T

IBM

Federal Reserve Board

Georgetown University

National Association of Public Utility Regulators

Pacific Gas & Electric

Thiokol Corporation

Association of American Railroads

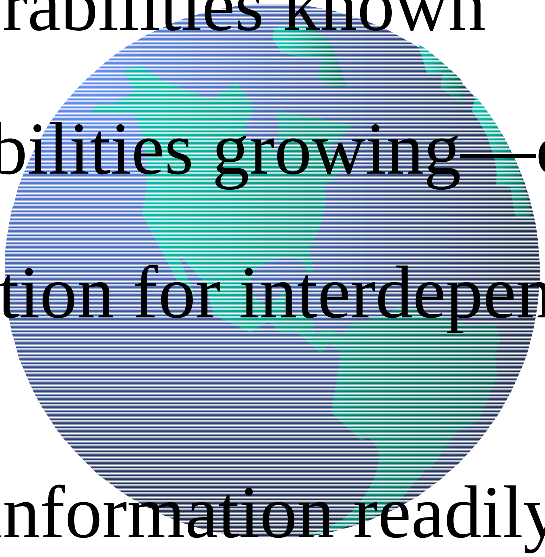
Outreach Efforts

- ♦ Public Meetings
  - *Atlanta, Boston, Houston, Los Angeles, St. Louis*
- ♦ Conferences
  - *Council on Competitiveness, Stanford University*
- ♦ Simulations
  - *Booz-Allen & Hamilton, Sandia National Laboratory*
- ♦ Approximately 6000 contacts
  - *Associations, corporations, government agencies*
- ♦ Media contacts
  - *Interviews, articles, broadcasts*
- ♦ World Wide Web page
  - *Speeches, meeting minutes, presentations*

Progress Report

- ♦ The Commission
- ♦ **Vulnerabilities and Threats**
- ♦ Findings
- ♦ Recommendations

Vulnerabilities



- Physical vulnerabilities known
- Cyber vulnerabilities growing—constantly changing
- Little appreciation for interdependencies and complexities
- Vulnerability information readily available

Threat

Threat = Capability + Intent

Capability = Skills + Tools

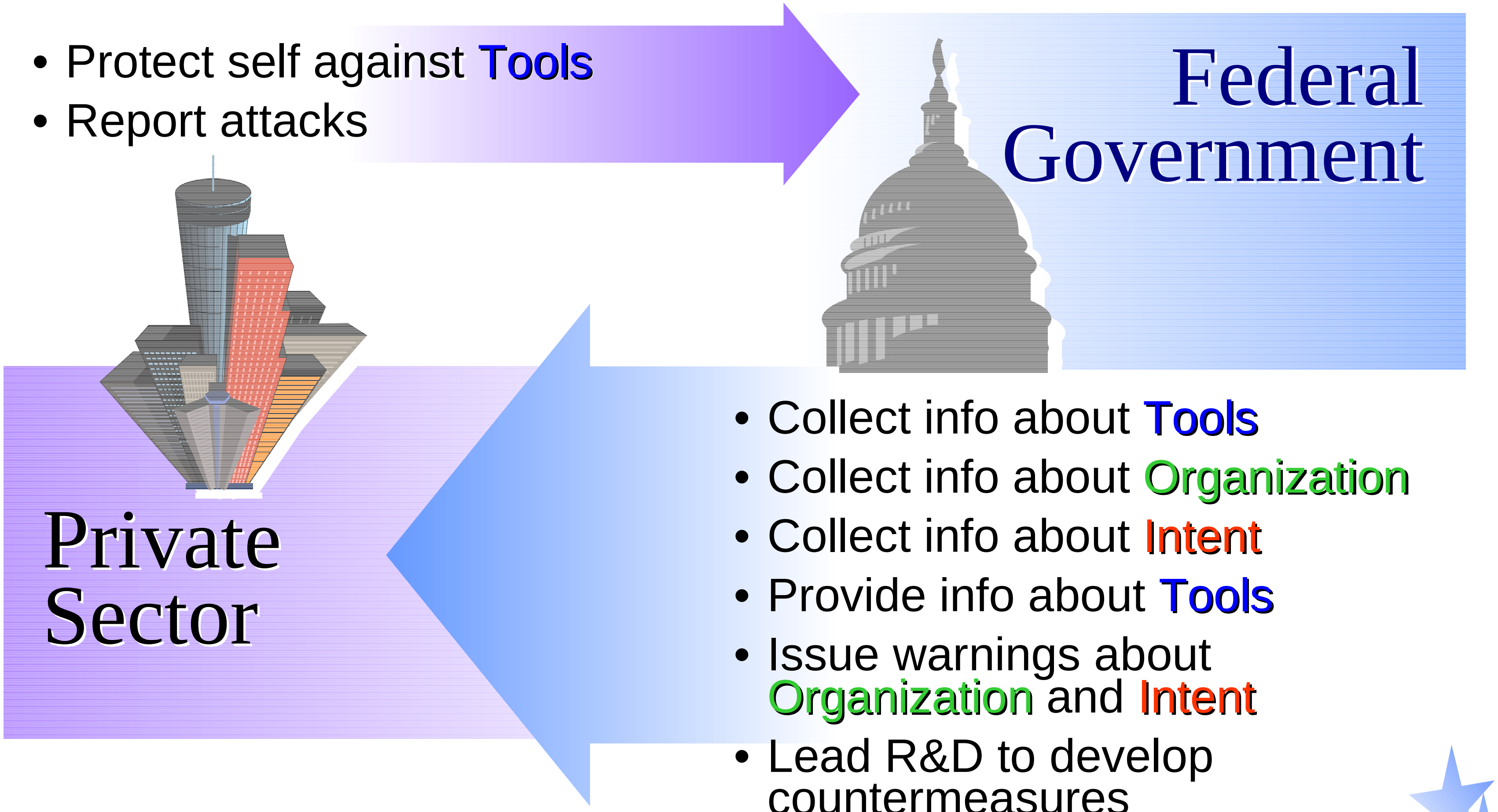
Tools = Equipment + Knowledge

Threat Spectrum

National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

INSIDERS

Responsibilities



- Protect self against Tools
- Report attacks

Federal Government

Private Sector

- Collect info about Tools
- Collect info about Organization
- Collect info about Intent
- Provide info about Tools
- Issue warnings about Organization and Intent
- Lead R&D to develop countermeasures

A New Arsenal

Cyber Intelligence

Anonymity

“Trojan Horses”

Denial of Service

Web Assaults

Data Theft

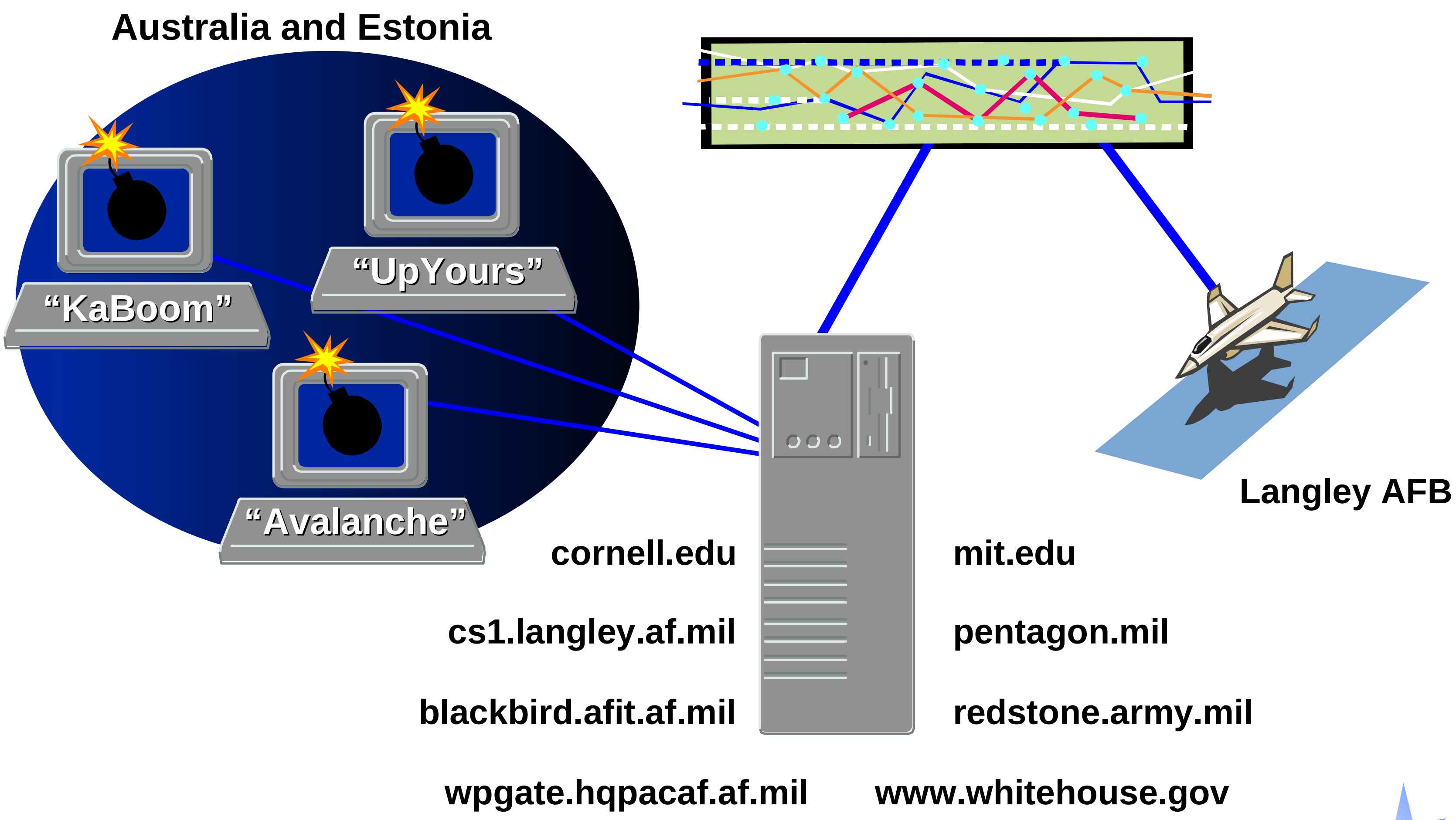
Viruses

Data Modification

E-Mail Attacks

Resource Abuse

E-mail Flooding



Australia and Estonia

“KaBoom”

“UpYours”

“Avalanche”

Langley AFB

cornell.edu

mit.edu

cs1.langley.af.mil

pentagon.mil

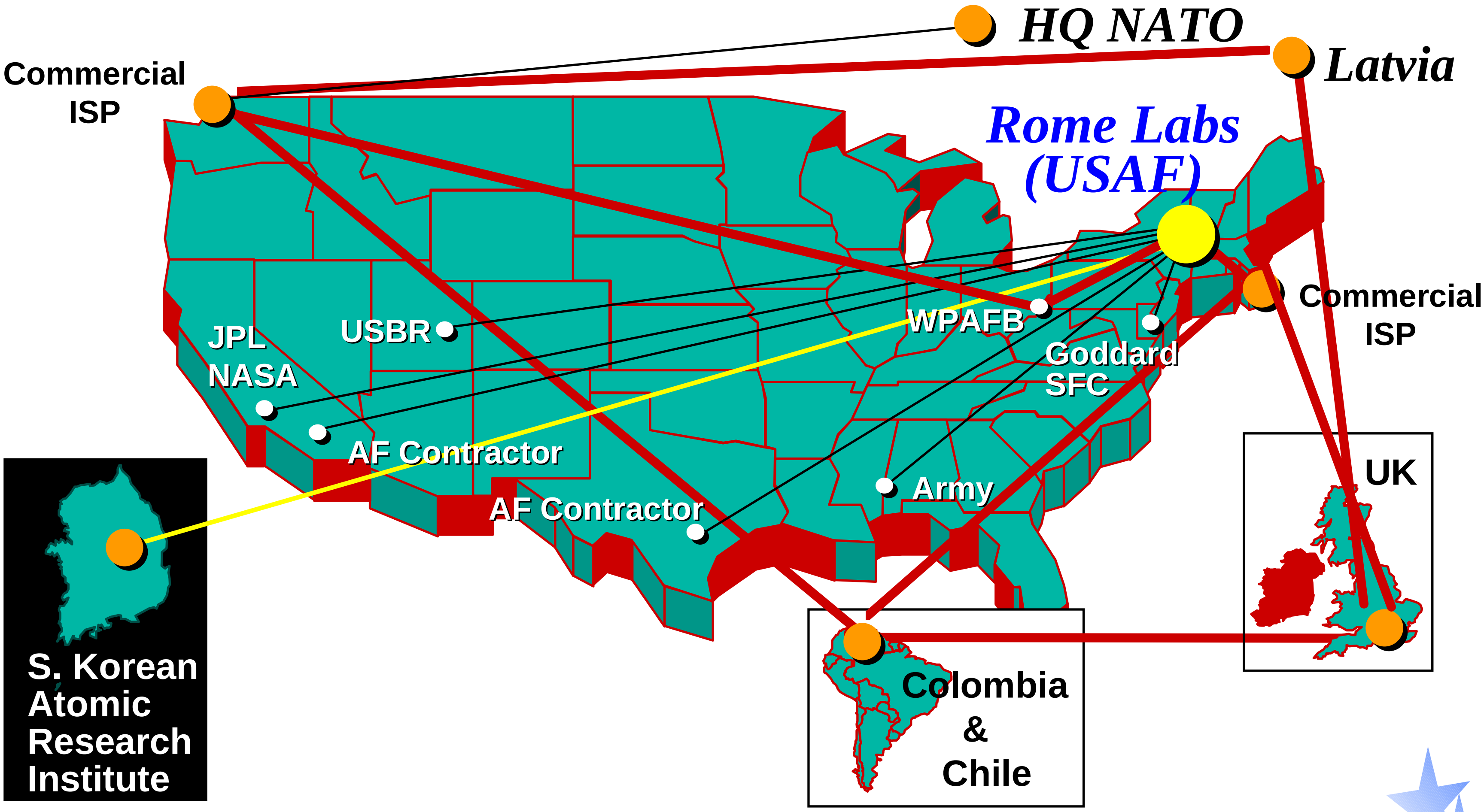
blackbird.afit.af.mil

redstone.army.mil

wpgate.hqpacaf.af.mil

www.whitehouse.gov

Intrusion


HQ NATO
Latvia
Commercial ISP
Rome Labs (USAF)
Commercial ISP
JPL NASA
USBR
WPAFB
Goddard SFC
AF Contractor
AF Contractor
Army
UK
S. Korean Atomic Research Institute
Colombia & Chile

Other Incidents

- Targeting
  - Penetrate computers for targeting information
- Loss of Service
  - Internet Service Providers
  - 911
  - Emergency Alerting System
- Theft
  - Credit Cards
  - Counterfeiting
  - Intellectual Property
  - Proprietary Data

Progress Report

- ♦ THE COMMISSION
- ♦ VULNERABILITIES AND THREATS
- ♦ **FINDINGS**
- ♦ RECOMMENDATIONS

Findings

- The challenge is adapting to a changing culture
- Vulnerabilities are serious and increasing
- Information sharing is the most immediate need
- National warning & analytic capabilities are lacking
- Government and industry are not prepared
- Legal framework needs modernization
- R&D and investment are not sufficient

Fundamental Conclusion

Risk is shared among public & private interests

Partnership is the Foundation for Infrastructure Protection

Progress Report

- The Commission
- Vulnerabilities and Threats
- Findings
- **Recommendations**

National Policy

- ♦ Critical infrastructures underpin American life
  - Deserve national attention and leadership
- ♦ US will assure availability/continuity
  - Defend by whatever means necessary
- ♦ Not just government or business responsibility
  - Partnership is required; specific federal responsibilities
- ♦ Urgent: establish national focal point
  - Public awareness
  - Infrastructure security and preparedness within Federal Government

Recommendations: Guiding Principles

- ♦ Government must lead by example
- ♦ Start with owners and operators
- ♦ Build on that which exists
- ♦ Promote voluntary cooperation
- ♦ Maintain existing oversight and regulation
- ♦ Practice continuous improvement

Recommendations: Information Sharing

***Objective:* Free interchange of essential threat and vulnerability information among all parties -- public and private.**

- Protect proprietary information
- Provide anonymity, as needed
- Ease anti-trust concerns
- Include state and local participants
- Establish sector "clearinghouses"
- Establish public-private information sharing and analysis center

Recommendations: Leading by Example

Objective: ***Federal government systems and processes serve as "benchmarks" for infrastructure assurance.***

- Use best practices
- Conduct certification
- Conduct information security pilot programs
- Address Global Positioning System vulnerability
- Emphasize security in National Airspace System design
- Acquire and retain cyber-qualified law enforcement personnel

Recommendations: Education & Awareness

***Objective:* Heightened awareness of critical infrastructure threats and vulnerabilities.**

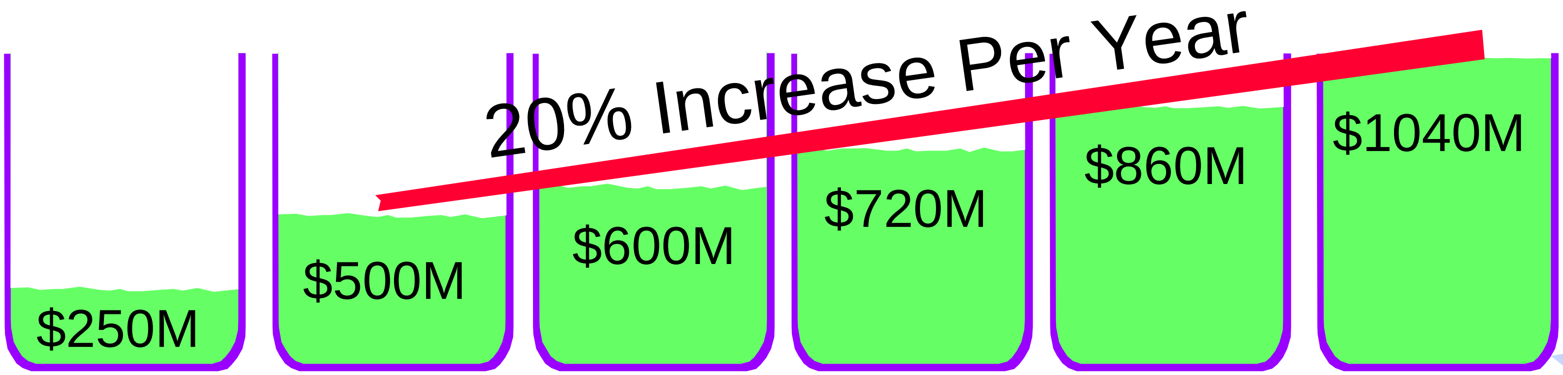
- Conduct White House conferences on computer ethics
- Conduct national awareness campaign
- Establish simulations and Round Tables
- National Science Foundation fund network security graduate programs
- Establish partnership between Department of Education and industry

Recommendations:

Research & Development

Objective: ***Tools and techniques for warning and protection.***

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



Recommendations:
Legal Initiatives

OBJECTIVES

- ✪ *Increased effectiveness of federal assurance and protection efforts*
- ✪ *Enhanced private sector ability to take protective action*
- ✪ *Assess impediments to partnership*

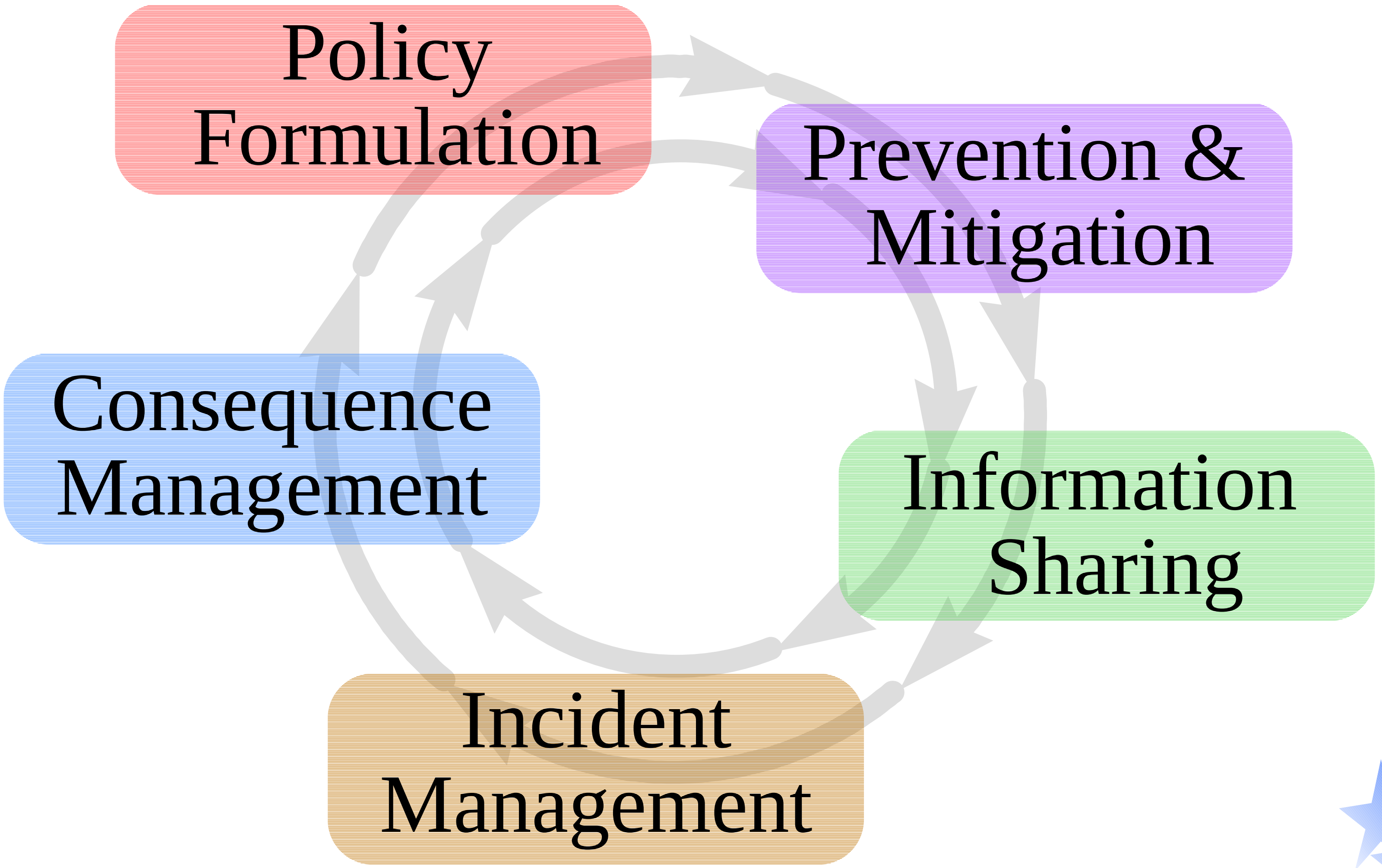
- ♦ Major Federal Legislation
- ♦ Criminal Law and Procedure
- ♦ Laws Governing Employer-Employee Relationship
- ♦ Legal Impediments to Information Sharing

Recommendations: Federal Assistance

***Objective:* Properly prepared owners and operators and state and local governments to accomplish their infrastructure protection roles.**

- NSA, DoE, DoD perform vulnerability risk assessments
- Encourage industry to develop risk methodologies
- Federal government review sensitive owner and operator information prior to publication
- Double Nunn-Lugar-Domenici funding

Infrastructure Assurance Functions



Policy Formulation

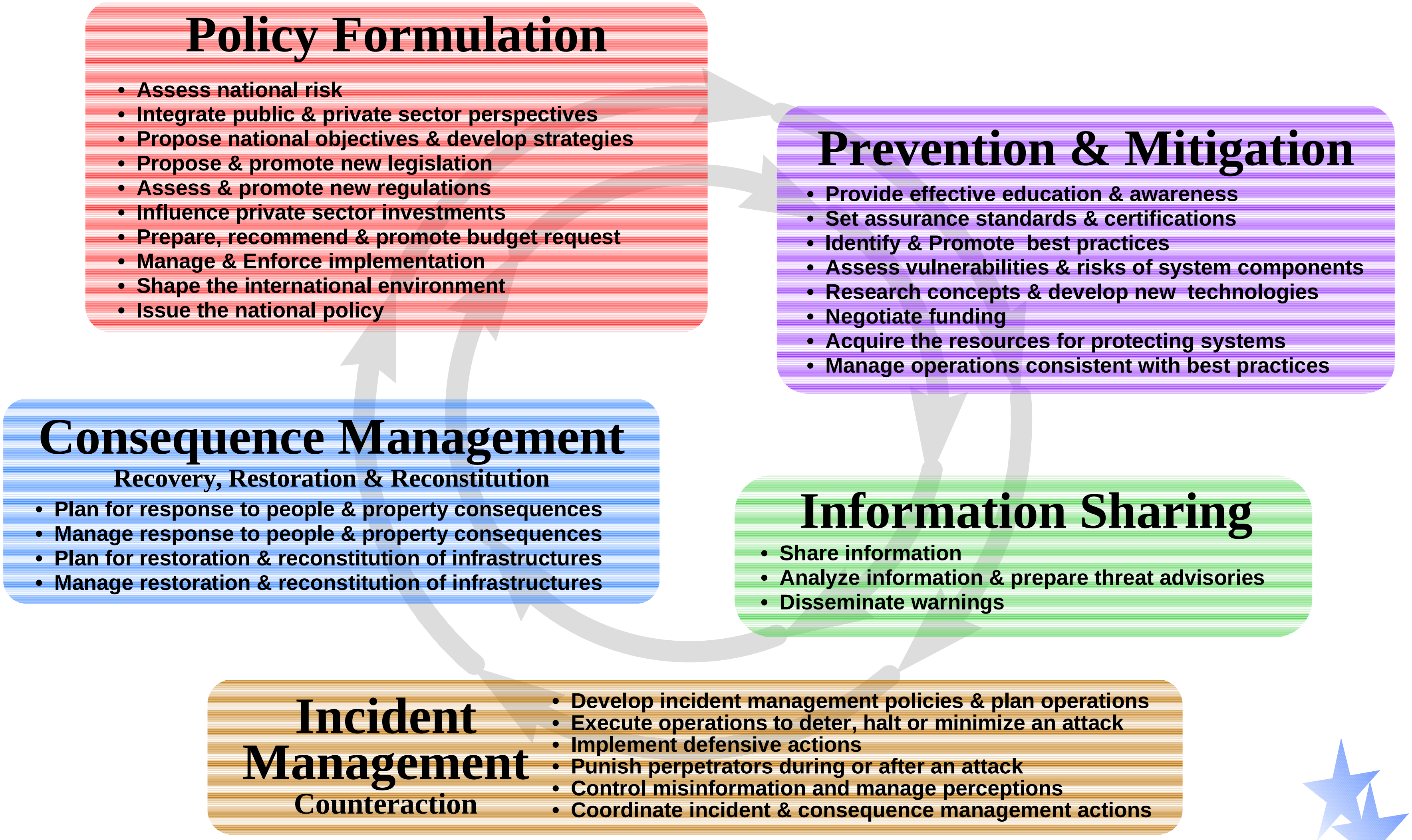
Prevention & Mitigation

Information Sharing

Incident Management

Consequence Management

Infrastructure Assurance Functions



Policy Formulation

- Assess national risk
- Integrate public & private sector perspectives
- Propose national objectives & develop strategies
- Propose & promote new legislation
- Assess & promote new regulations
- Influence private sector investments
- Prepare, recommend & promote budget request
- Manage & Enforce implementation
- Shape the international environment
- Issue the national policy

Prevention & Mitigation

- Provide effective education & awareness
- Set assurance standards & certifications
- Identify & Promote best practices
- Assess vulnerabilities & risks of system components
- Research concepts & develop new technologies
- Negotiate funding
- Acquire the resources for protecting systems
- Manage operations consistent with best practices

Information Sharing

- Share information
- Analyze information & prepare threat advisories
- Disseminate warnings

Incident Management

Counteraction

- Develop incident management policies & plan operations
- Execute operations to deter, halt or minimize an attack
- Implement defensive actions
- Punish perpetrators during or after an attack
- Control misinformation and manage perceptions
- Coordinate incident & consequence management actions

Consequence Management

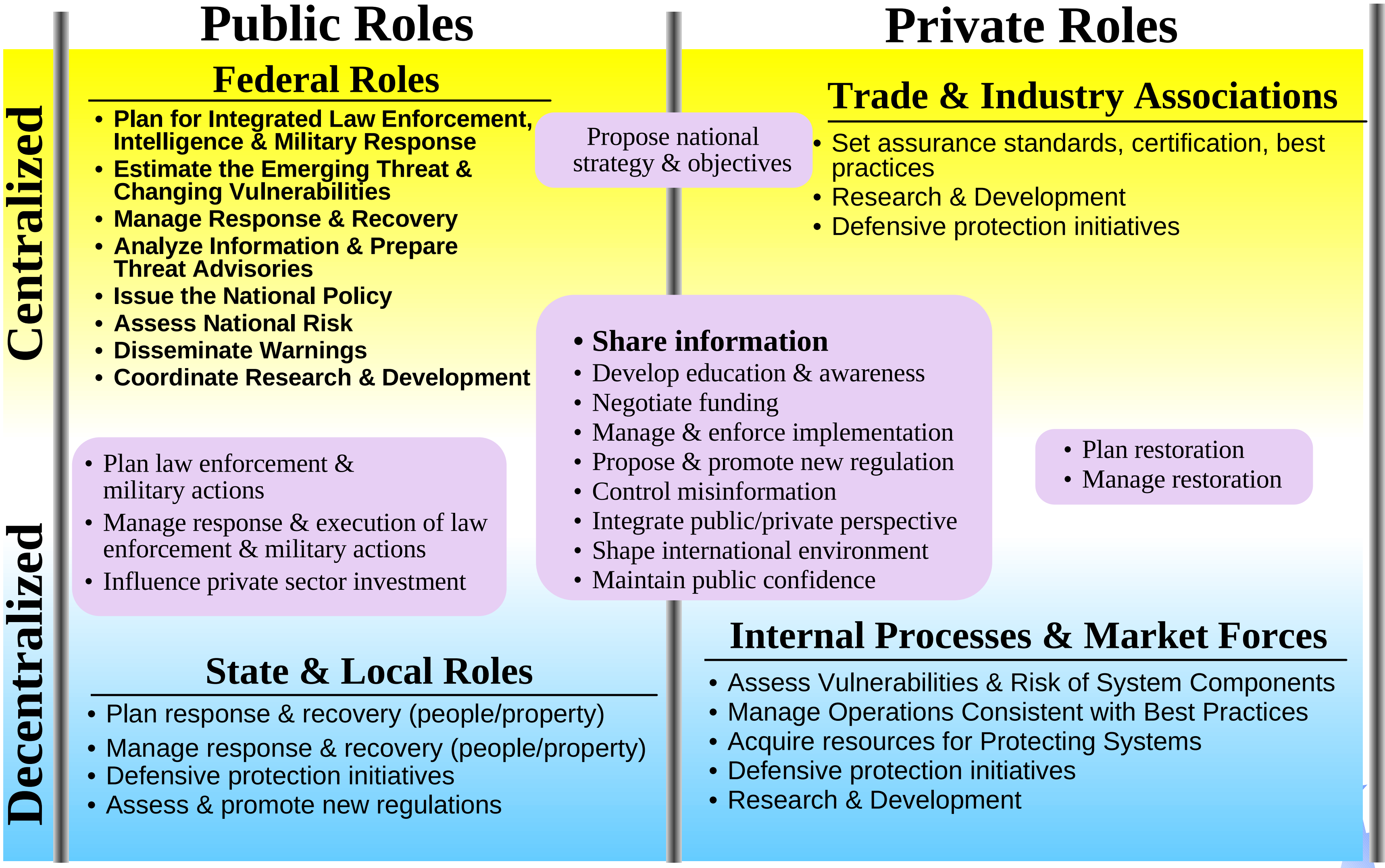
Recovery, Restoration & Reconstitution

- Plan for response to people & property consequences
- Manage response to people & property consequences
- Plan for restoration & reconstitution of infrastructures
- Manage restoration & reconstitution of infrastructures

“Location” of Roles In Infrastructure Assurance

	Public Roles	Private Roles
Centralized	Federal Roles	Trade & Industry Associations
	State Roles	
		Companies
Decentralized	Local Roles	Internal Processes & Market Forces

"Location" of *Functions* in Infrastructure Assurance



Public Roles

Private Roles

Centralized

Decentralized

Federal Roles

- **Plan for Integrated Law Enforcement, Intelligence & Military Response**
- **Estimate the Emerging Threat & Changing Vulnerabilities**
- **Manage Response & Recovery**
- **Analyze Information & Prepare Threat Advisories**
- **Issue the National Policy**
- **Assess National Risk**
- **Disseminate Warnings**
- **Coordinate Research & Development**

Propose national strategy & objectives

Trade & Industry Associations

- Set assurance standards, certification, best practices
- Research & Development
- Defensive protection initiatives

- **Share information**
- Develop education & awareness
- Negotiate funding
- Manage & enforce implementation
- Propose & promote new regulation
- Control misinformation
- Integrate public/private perspective
- Shape international environment
- Maintain public confidence

- Plan law enforcement & military actions
- Manage response & execution of law enforcement & military actions
- Influence private sector investment

- Plan restoration
- Manage restoration

State & Local Roles

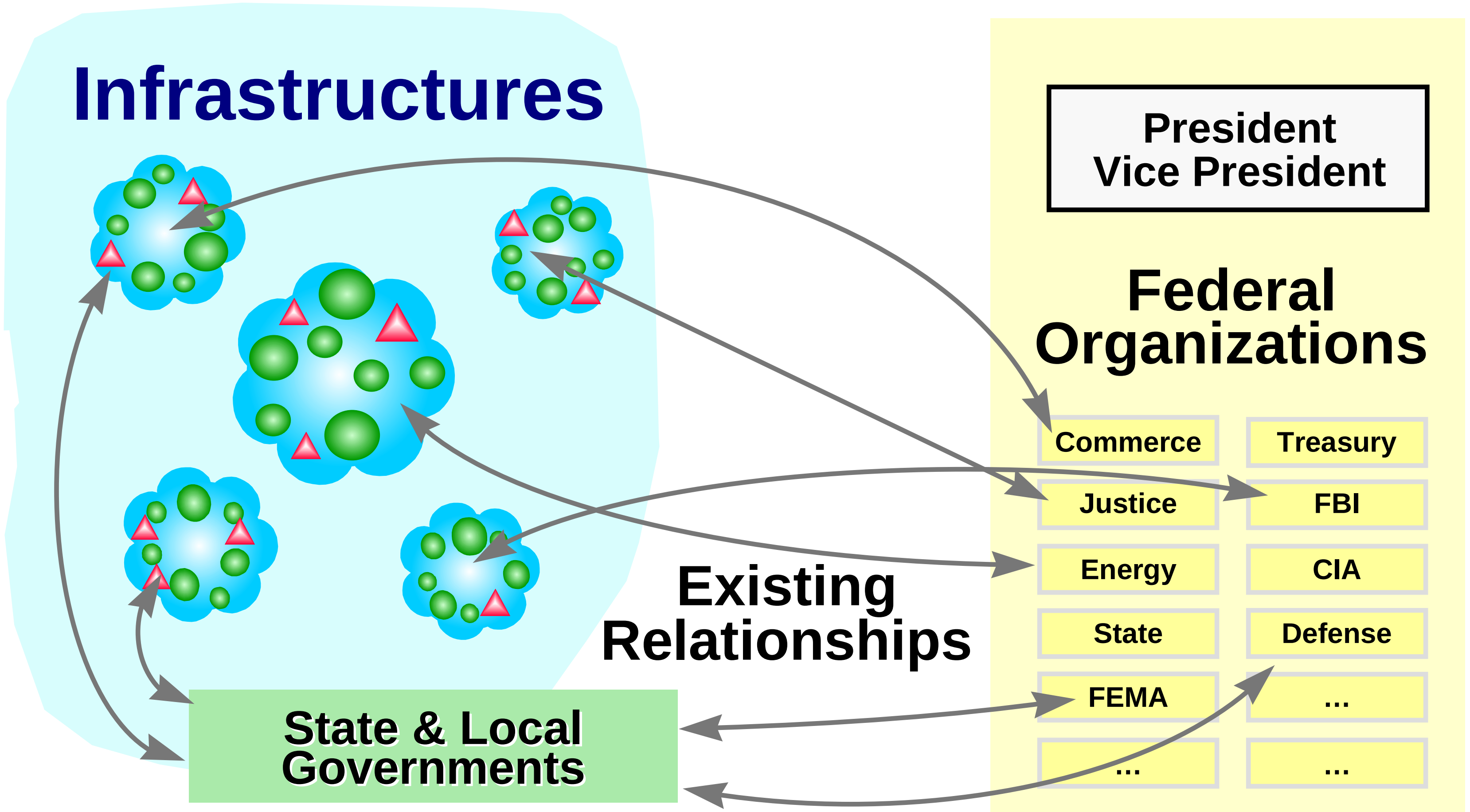
- Plan response & recovery (people/property)
- Manage response & recovery (people/property)
- Defensive protection initiatives
- Assess & promote new regulations

Internal Processes & Market Forces

- Assess Vulnerabilities & Risk of System Components
- Manage Operations Consistent with Best Practices
- Acquire resources for Protecting Systems
- Defensive protection initiatives
- Research & Development

1997

Infrastructure Assurance: *Today*



Infrastructures

President
Vice President

Federal Organizations

Commerce	Treasury
Justice	FBI
Energy	CIA
State	Defense
FEMA	...
...	...

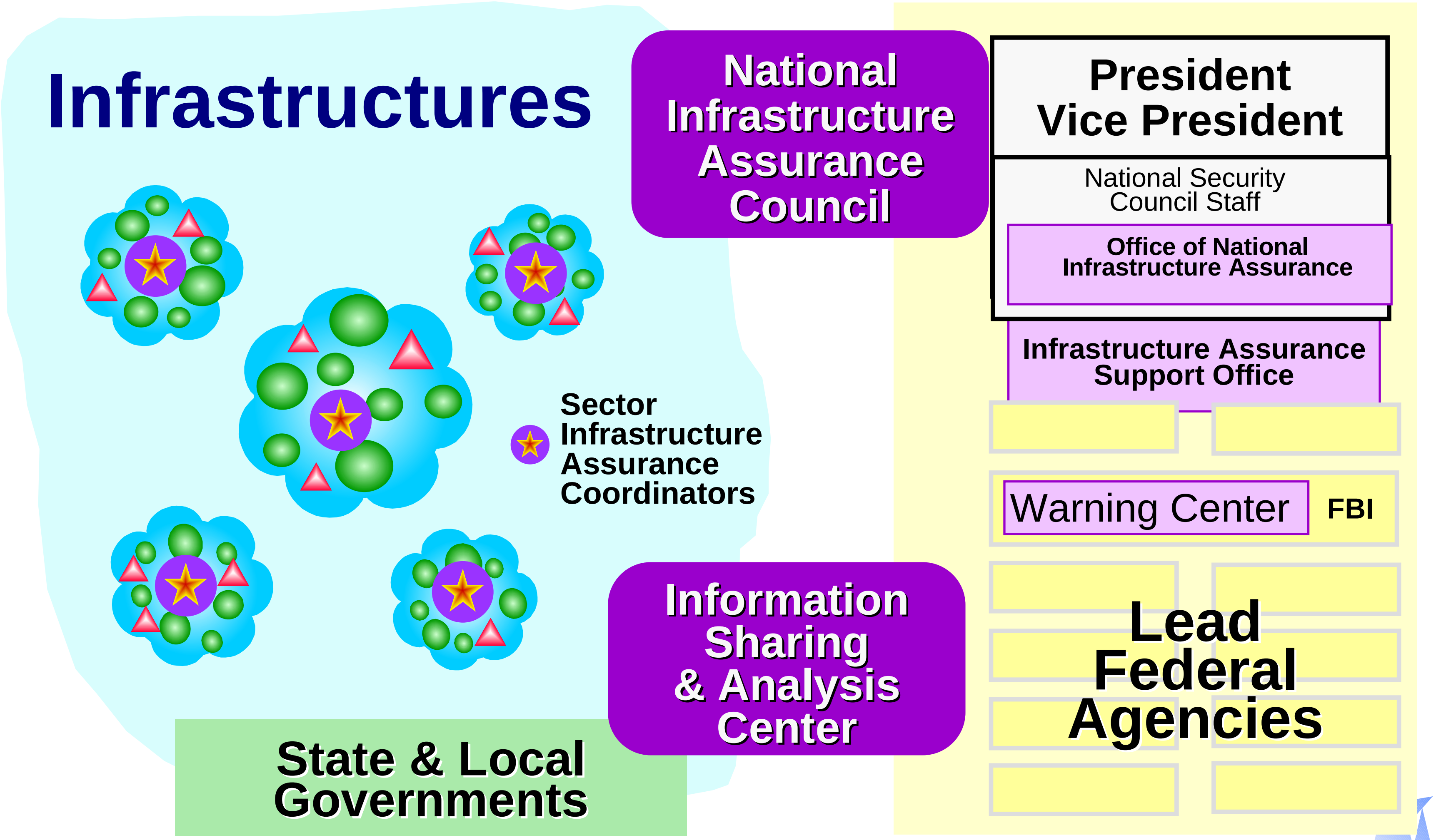
Existing Relationships

State & Local Governments

● Owners & Operators

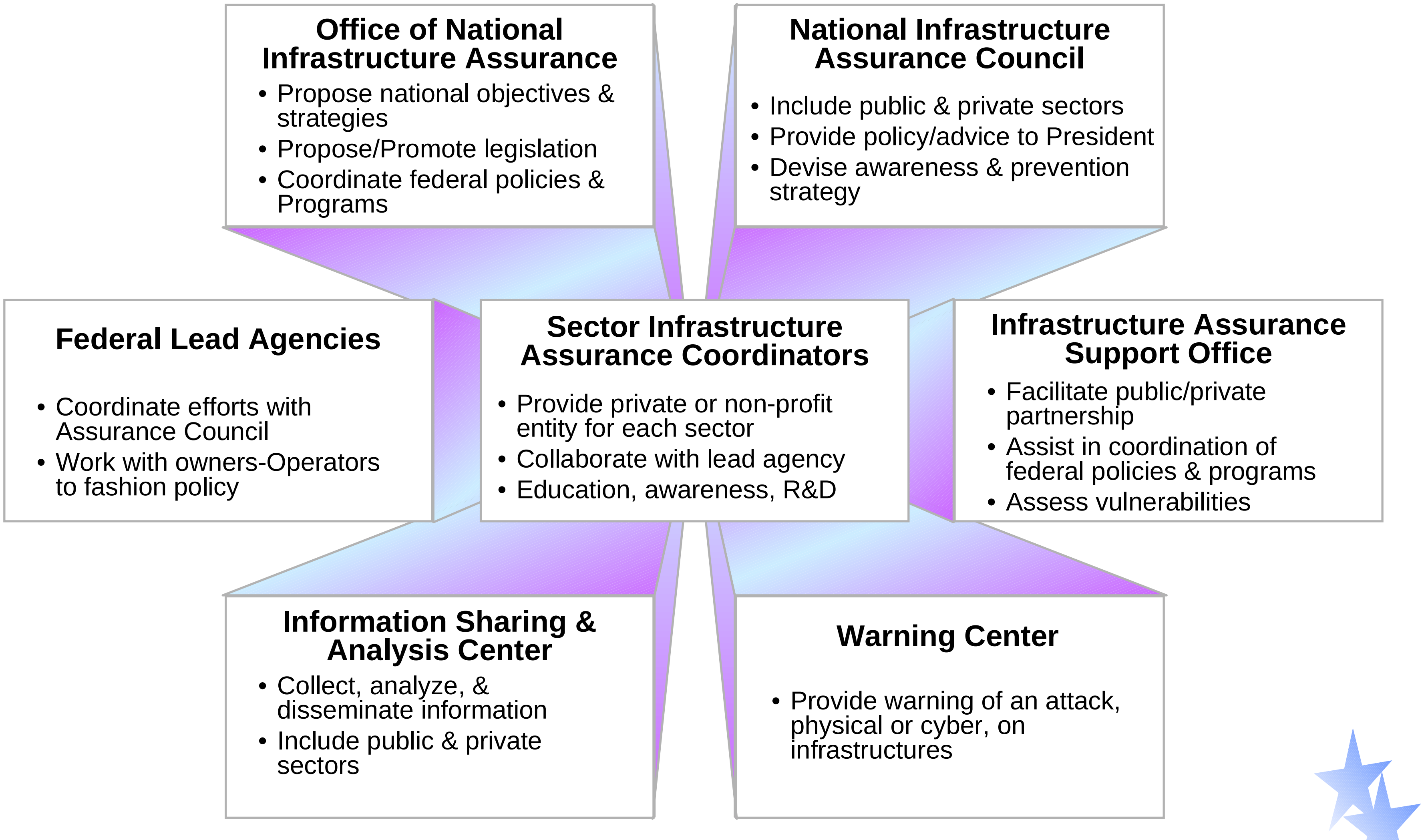
▲ Associations, Consortia

Infrastructure Assurance: *Proposed*



Infrastructures
National Infrastructure Assurance Council
President
Vice President
National Security Council Staff
Office of National Infrastructure Assurance
Infrastructure Assurance Support Office
Sector Infrastructure Assurance Coordinators
Warning Center
FBI
Information Sharing & Analysis Center
Lead Federal Agencies
State & Local Governments

Proposed National Structure



Office of National Infrastructure Assurance

- Propose national objectives & strategies
- Propose/Promote legislation
- Coordinate federal policies & Programs

National Infrastructure Assurance Council

- Include public & private sectors
- Provide policy/advice to President
- Devise awareness & prevention strategy

Federal Lead Agencies

- Coordinate efforts with Assurance Council
- Work with owners-Operators to fashion policy

Sector Infrastructure Assurance Coordinators

- Provide private or non-profit entity for each sector
- Collaborate with lead agency
- Education, awareness, R&D

Infrastructure Assurance Support Office

- Facilitate public/private partnership
- Assist in coordination of federal policies & programs
- Assess vulnerabilities

Information Sharing & Analysis Center

- Collect, analyze, & disseminate information
- Include public & private sectors

Warning Center

- Provide warning of an attack, physical or cyber, on infrastructures

Conclusion

Risk is shared among public & private interests

Partnership is the Foundation for Infrastructure Protection