Homeland Security Policy Council

Federal Communications Commission

Amal Abdallah
Senior Attorney
International Bureau
Federal Communications Commission

Homeland Security Sectors

Agriculture Banking and Finance Chemical Industry

Defense Industrial Base Emergency Services Energy

Food Government

Information and Telecommunications Postal and Shipping

Water

Transportation

Public Health

- All other sectors rely on the Information and Telecommunications sector

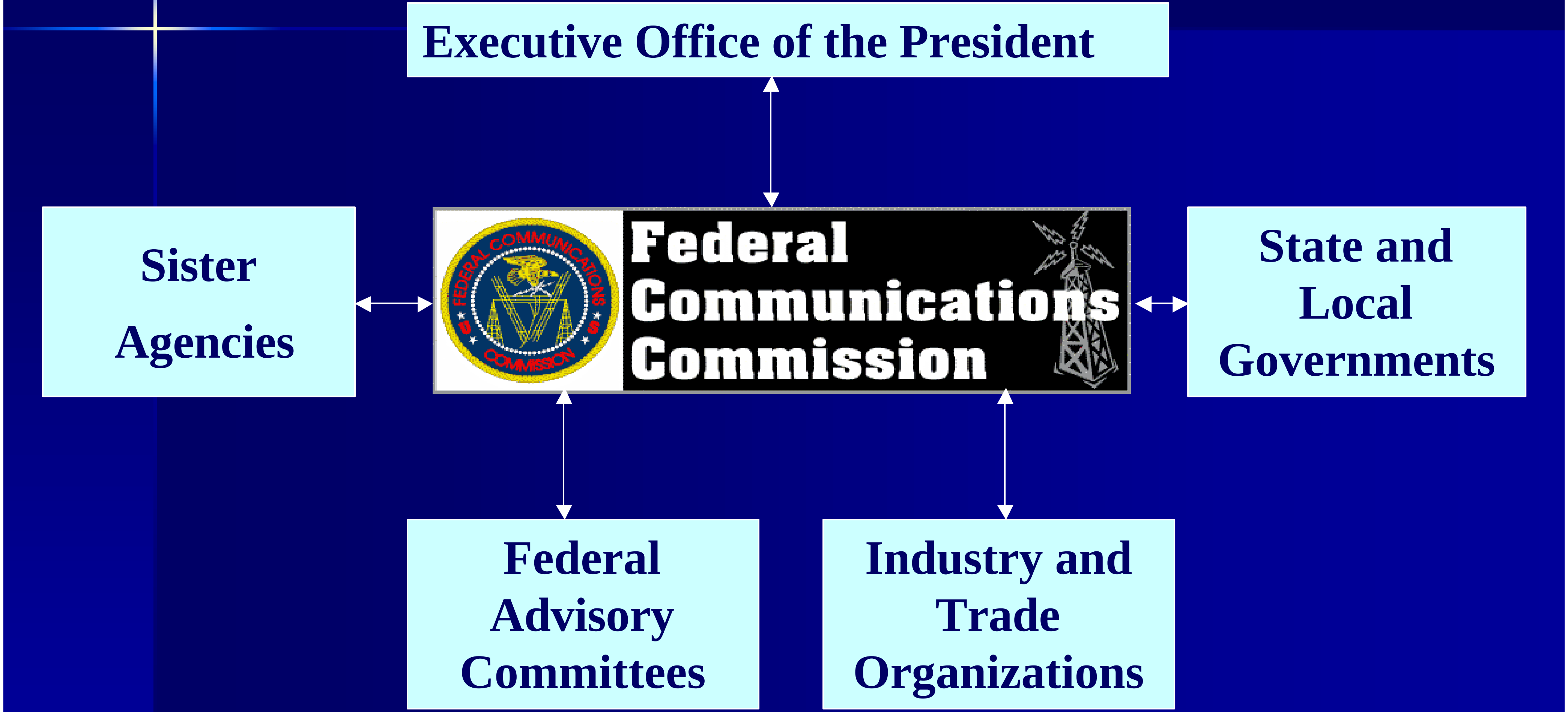
FCC's Homeland Security Mission

- Evaluate and strengthen measures for protecting the Nation's communications infrastructure.
- Facilitate rapid restoration of that infrastructure in the event of disruption.
- Develop policies that promote access to effective communications services by public safety, public health, and other emergency personnel in emergency situations.

FCC’s Homeland Security Focus

- Interagency and Industry Partnerships
- Infrastructure Protection
- Communications Reliability
- Public Safety Communications
- Spectrum Policy
- New Technologies

FCC's Homeland Security Partnerships



Executive Office of the President

Sister Agencies

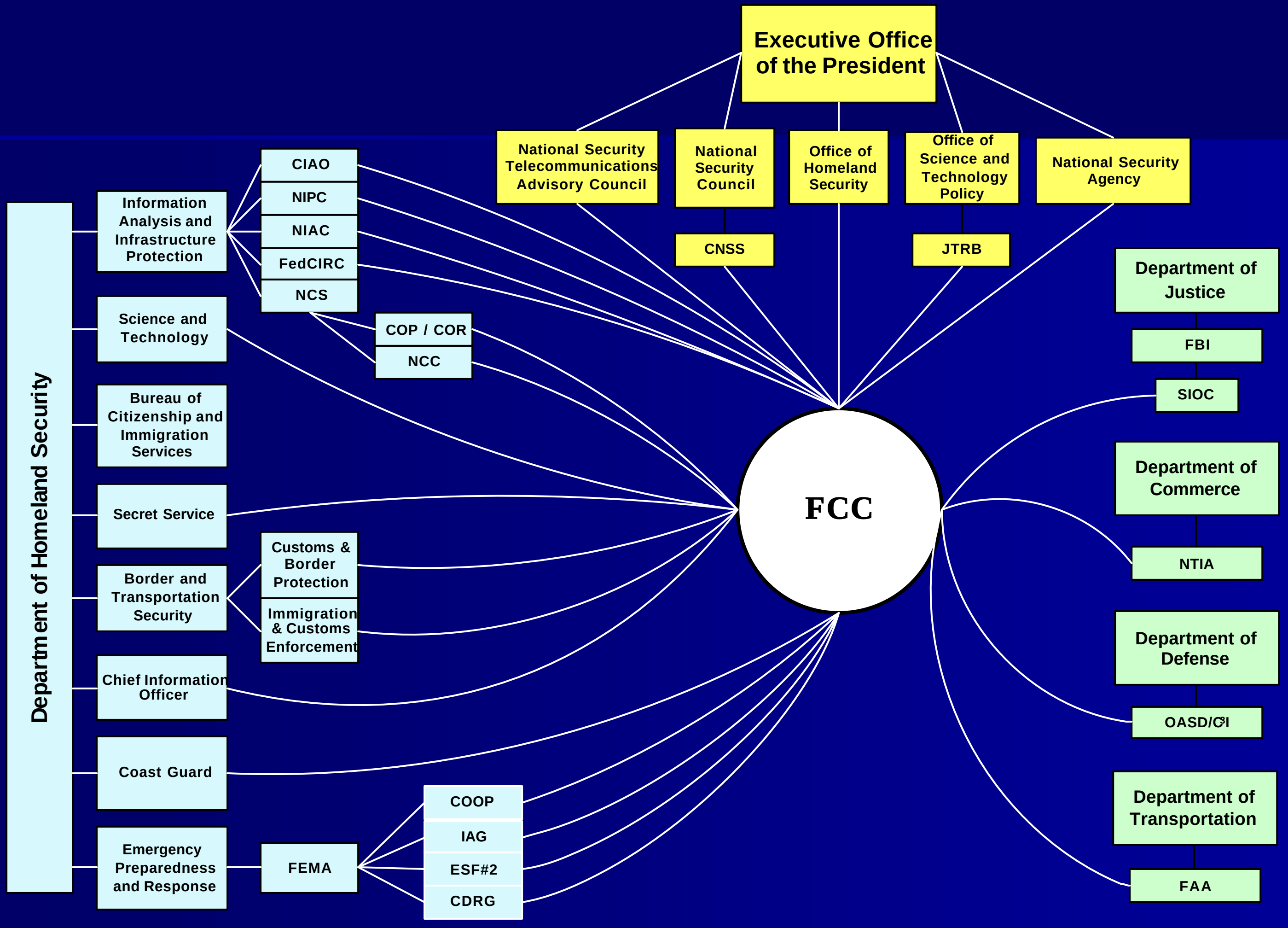
Federal Communications Commission

State and Local Governments

Federal Advisory Committees

Industry and Trade Organizations

Interagency Efforts: View from the FCC



Executive Office of the President

National Security Telecommunications Advisory Council

National Security Council

CNSS

Office of Homeland Security

Office of Science and Technology Policy

JTRB

National Security Agency

FCC

Department of Homeland Security

Information Analysis and Infrastructure Protection

CIAO

NIPC

NIAC

FedCIRC

NCS

COP / COR

NCC

Science and Technology

Bureau of Citizenship and Immigration Services

Secret Service

Border and Transportation Security

Customs & Border Protection

Immigration & Customs Enforcement

Chief Information Officer

Coast Guard

Emergency Preparedness and Response

FEMA

COOP

IAG

ESF#2

CDRG

Department of Justice

FBI

SIOC

Department of Commerce

NTIA

Department of Defense

OASD/C^{3}I

Department of Transportation

FAA

FCC Partnership with NCS/NCC

- The National Communications System (NCS) continues to be our strongest partner in our efforts to coordinate industry response to a network outage or attack.

- FCC is assisting NCS in promoting its efforts to improve emergency communications through the Telecommunications Service Priority (TSP), Government Emergency Telecommunications System (GETS) and Wireless Priority Access (WPAS) programs.

Infrastructure Protection

- FCC rechartered our Network Reliability and Interoperability Council (NRIC VI) federal advisory committee in January 2002 to focus on homeland security issues. (www.nric.org)
- FCC created a new Media Security and Reliability Council (MSRC) federal advisory committee in March 2002 to address broadcast, cable and satellite homeland security issues. (www.mediasecurity.org)

Network Reliability and Interoperability Council

- First chartered in 1993. NRIC has a 10-year history of improving network reliability.
- Expanded membership in 2001 charter.
- December 2002 - Delivered best practices for securing the physical and cyber networks.
- March 2002 - Delivered best practices for service restoration and disaster recovery.

NRIC VI Charter

- Establish industry Best Practices to address external threats to communications infrastructure.
- Build on the reliability and interoperability work of previous NRICs by expanding membership to include more industry segments.

Principles for Developing Best Practices

1. “People Implement Best Practices"
2. Do *not* endorse commercial or specific "pay for" documents, products or services
3. Address classes of problems
4. Already implemented
5. Developed by industry consensus
6. Best Practices are verified by a broader set of industry members
7. Sufficient rigor and deliberation

Principles for Implementing and Maintaining Best Practices (*See*, www.nric.org)

- Current list of best practices (BPs) are constrained by what can be implemented
- Not all BPs are appropriate for all service providers or architectural implementations
- The BPs are not intended for mandatory regulatory efforts
- This is a moving target that will require ***continual*** refinement, additions and improvement

NRIC VI Focus Group Structure

Focus Group 1 Homeland Security

A. **Physical Security**

B. **Cyber Security**

C. **Public Safety**

D. **Disaster Recovery and Mutual Aid**

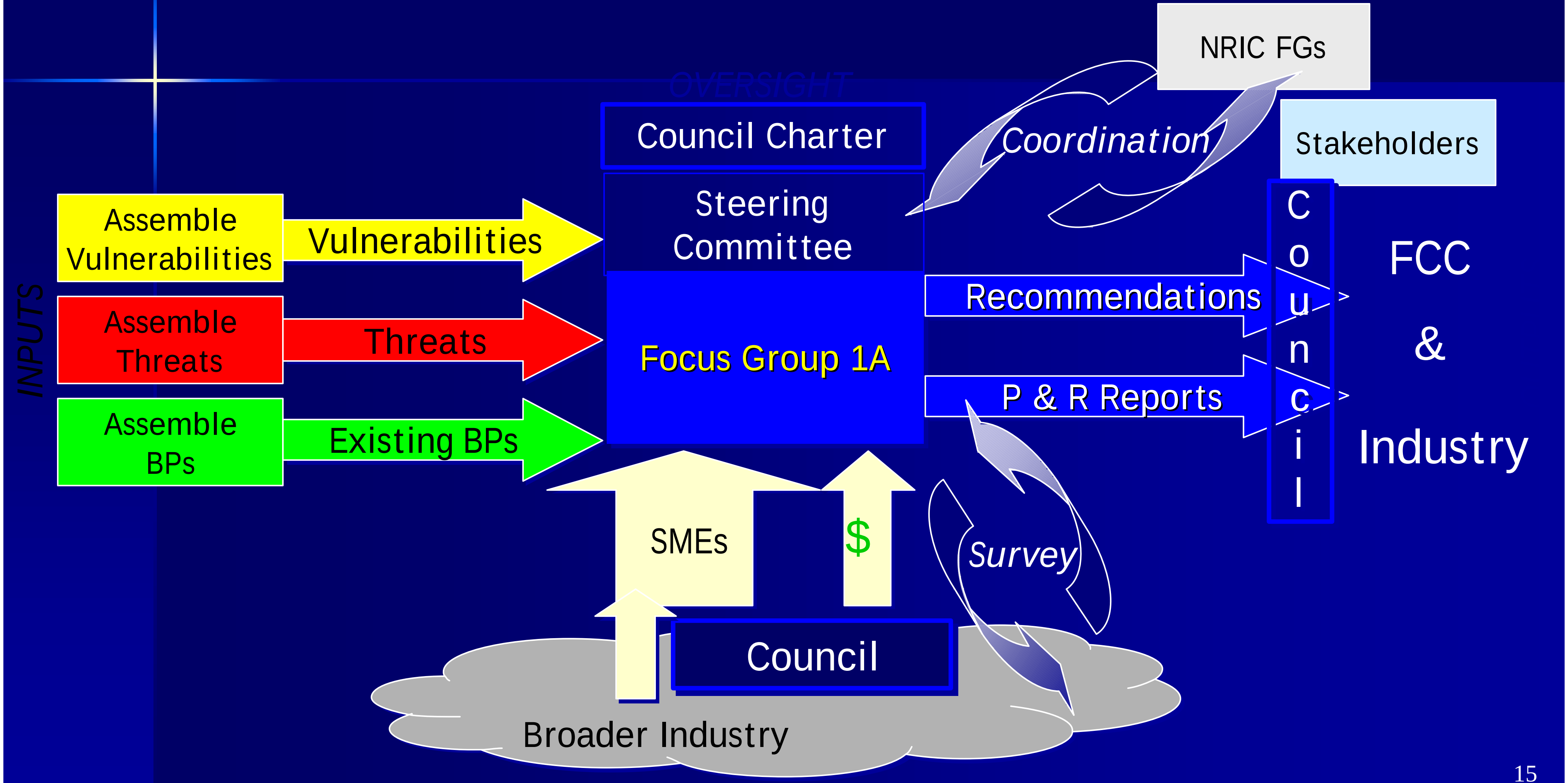
Focus Group 2 Network Reliability

Focus Group 3 Network Interoperability

Focus Group 4 Broadband

NRIC VI Physical Security Focus Group

Big Picture of Process Flow



INPUTS

Assemble Vulnerabilities

Vulnerabilities

Assemble Threats

Threats

Assemble BPs

Existing BPs

OVERSIGHT

Council Charter

Steering Committee

Focus Group 1A

SMEs

$

Council

Broader Industry

NRIC FGs

Coordination

Stakeholders

Recommendations

P & R Reports

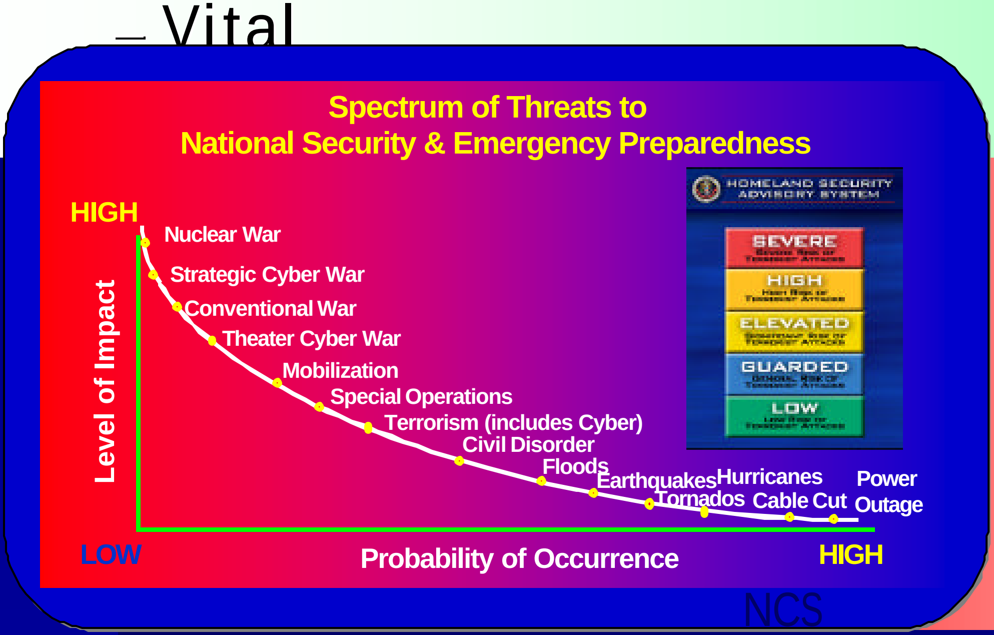
Survey

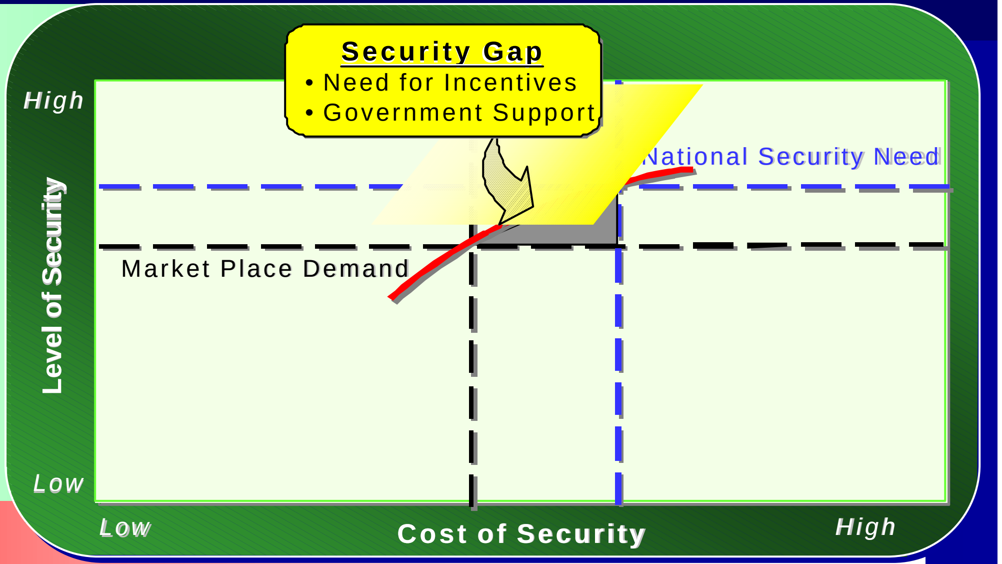
Council

FCC & Industry

The Need for Physical Security Best Practices

- Communications Infrastructure is
  - Vast
  - Very Complex
  - Vital

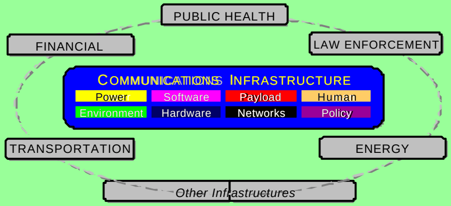




- Terrorist Threats Exist
  - Target
  - Train
    - plan
    - patient
    - persistent

Environment

Environment – includes buildings, trenches where cables are buried, space where satellites orbit, the ocean where submarine cables reside



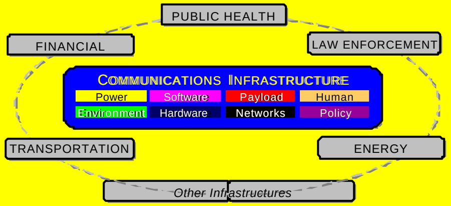
Areas for Attention

1. Need for Periodic Re-Assessment
2. Any Environment Can Be Destroyed
3. Unique Circumstances Require Special Consideration
4. Overall Security Plan

Example Best Practice (6-P-5190)
Access to critical areas within Telecom Hotels where Service Providers and Network Operators share common space should be restricted to personnel with a jointly agreed upon need for access.

Power

Power – includes the internal power infrastructure, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel



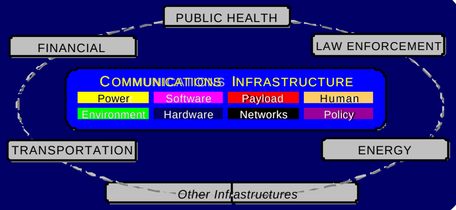
Areas for Attention

1. Internal Power Infrastructure Is Often Overlooked
2. Rules Permitting Access to Internal Power Systems Increase Risk Priorities for Good Power Systems Management Compete with Environmental Concerns
3. Power System Competencies Needs to Be Maintained

Example Best Practice (6-P-5207): Service Providers and Network Operators should take appropriate precautions at critical installations to ensure that fuel supplies and alternate sources are available in the event of major disruptions in a geographic area (e.g., hurricane, earthquake, pipeline disruption).

Hardware

Hardware – includes the hardware frames, electronics circuit packs and cards, metallic and fiber optic transmission cables and semiconductor chips



Areas for Attention

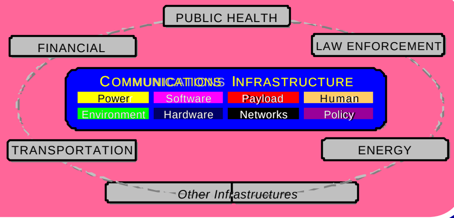
1. **Nuclear Attack**
2. **Hardness to Radiation**
3. **Solar Flares and Coronal Mass Ejection**

Example Best Practice (6-P-5118)

Equipment Suppliers of critical network elements should test electronic hardware to ensure its compliance with appropriate electromagnetic energy tolerance criteria for electromagnetic energy, shock, vibration, voltage spikes, and temperature.

Software

Software – includes the physical storage of software releases, development and test loads, version control and management, chain of control delivery



Areas for Attention

1. Physical Security of Software

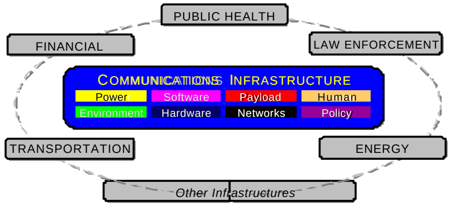
*(*Cyber Security)*

Example Best Practice (6-P-5167)

Equipment Suppliers should provide secured methods, both physical and electronic, for the internal distribution of software development and production materials.

Networks

Networks – includes the configuration of nodes, various types of networks, technology, synchronization, redundancy, and physical and logical diversity



Areas for Attention

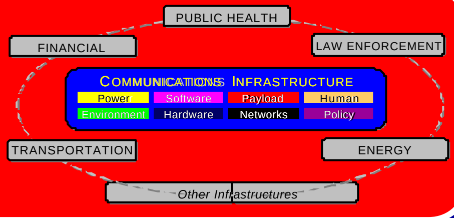
1. **Network Redundancy and Diversity**
2. **Existing NRIC Best Practices Effectively Address Networks Vulnerabilities**

Example Best Practice (6-P-5107)

Service Providers and Network Operators should develop a comprehensive plan to evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with the concentration of infrastructure components.

Payload

Payload – includes the information transported across the infrastructure, traffic patterns and statistics, information interception and information corruption



Areas for Attention

1. Physical Aspects of Securing Network Payload

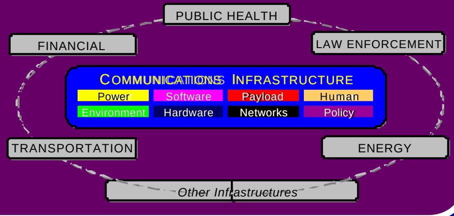
*(*Cyber Security)*

Example Best Practice (6-P-5173)

Network Operators and Equipment Suppliers should design wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) to minimize the potential for interception.

Policy

Policy – includes the industry standards, industry cooperation, industry interfaces with governments (local, state, federal), and various legal issues



Areas for Attention

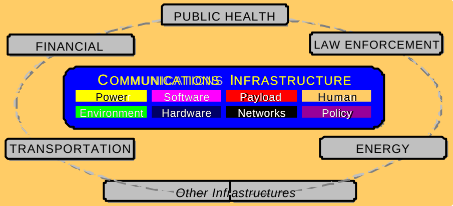
1. **Inadvertent Negative Impact of Government Regulations**
2. **FCC Effects on Vulnerabilities and Best Practices**

Example Best Practice (6-P-5157)

Appropriate corporate personnel (within Service Providers, Network Operators, Equipment Suppliers and the Government organizations) should implement a process for reviewing government, state, local filings and judicial proceeding for impact on revealing vulnerabilities of critical infrastructure.

Human

Human – includes intentional and unintentional behaviors, limitations, and education and training, human-machine interfaces, and ethics



Areas for Attention

1. **Complex Interactions**

Example Best Practice (6-P-5176)

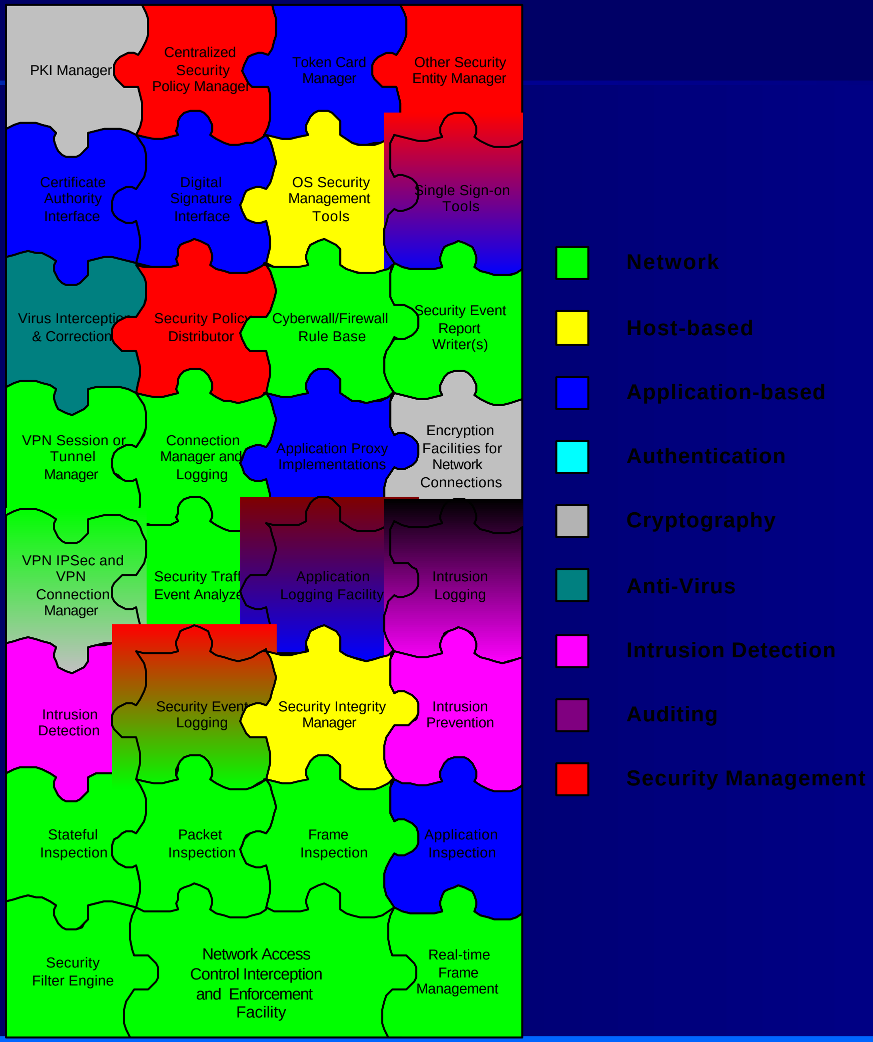
Service Providers, Network Operators and Equipment Suppliers should consider establishing an employee awareness training program to ensure that employees who create, receive or transfer proprietary information are aware of their responsibilities for compliance with proprietary information protection policy and procedures.

NRIC VI Cybersecurity Focus Group

Charter of Cybersecurity Focus Group

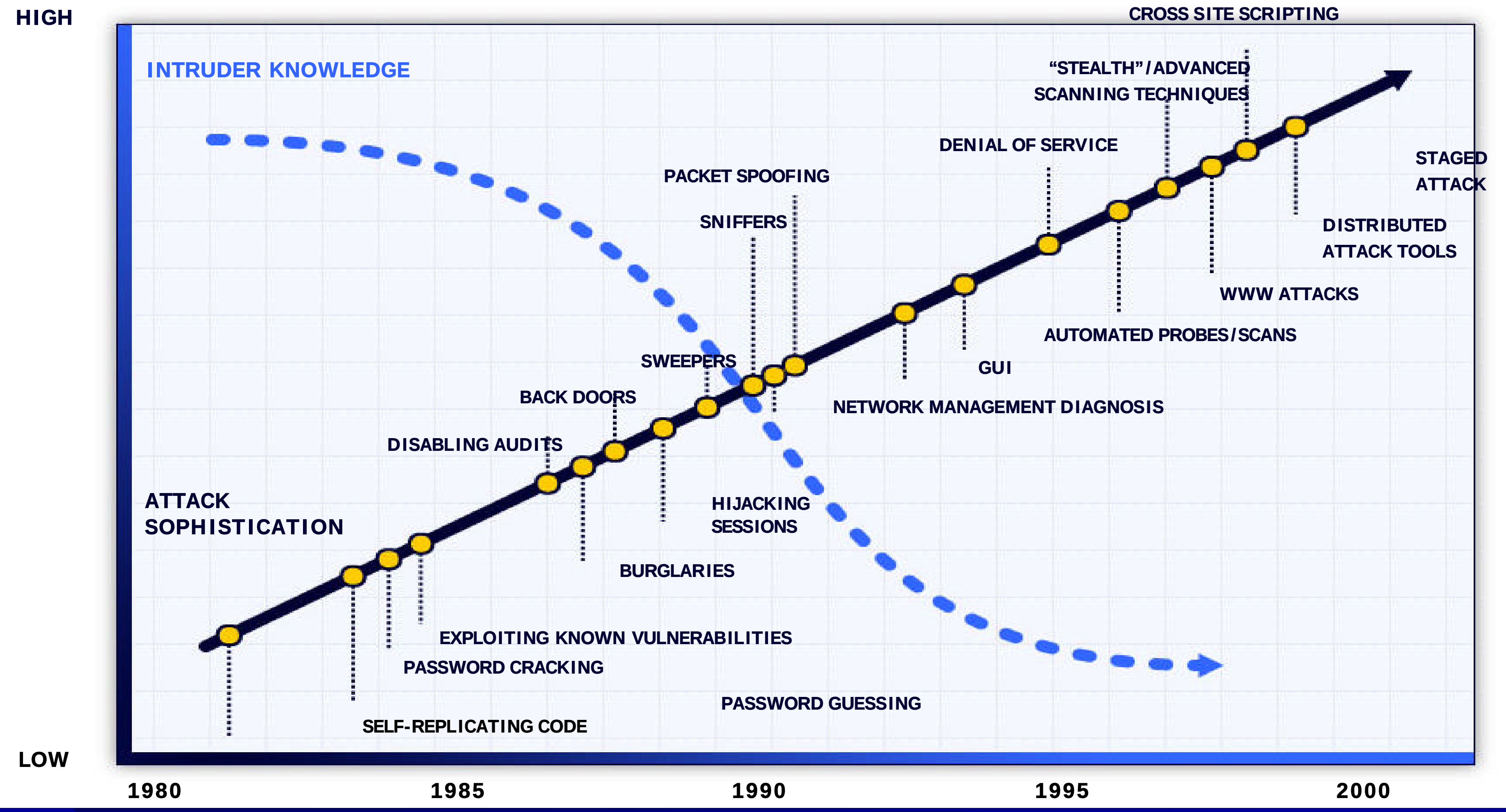
- Generate Best Practices for cybersecurity (*see*, http://www.nric.org/fg/nricvifg.html)
- Telecommunications sector
  - Internet services
- Deliverables
  - December 2002 – prevention
  - March 2003 – recovery
- New team, limited baseline material

Security is Very Complex

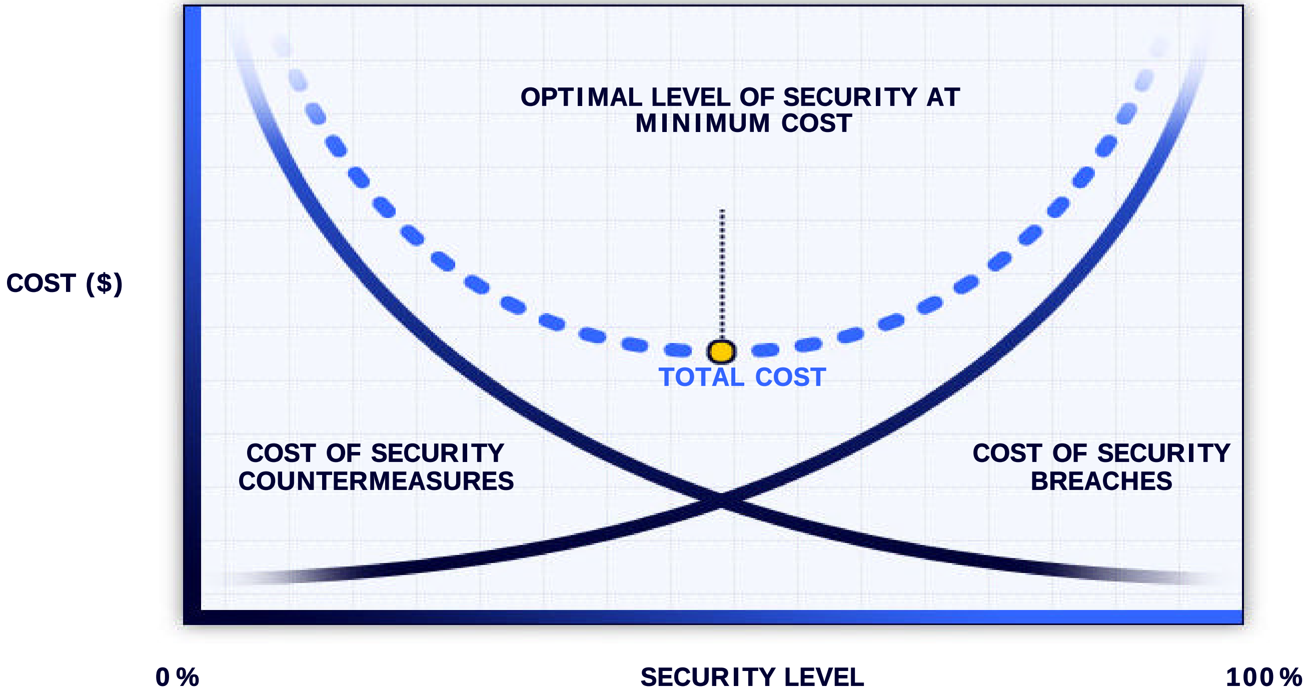

PKI Manager
Centralized Security Policy Manager
Token Card Manager
Other Security Entity Manager
Certificate Authority Interface
Digital Signature Interface
OS Security Management Tools
Single Sign-on Tools
Virus Interception & Correction
Security Policy Distributor
Cyberwall/Firewall Rule Base
Security Event Report Writer(s)
VPN Session or Tunnel Manager
Connection Manager and Logging
Application Proxy Implementations
Encryption Facilities for Network Connections
VPN IPSec and VPN Connection Manager
Security Traffic Event Analyzer
Application Logging Facility
Intrusion Logging
Intrusion Detection
Security Event Logging
Security Integrity Manager
Intrusion Prevention
Stateful Inspection
Packet Inspection
Frame Inspection
Application Inspection
Security Filter Engine
Network Access Control Interception and Enforcement Facility
Real-time Frame Management
🟩 Network
🟨 Host-based
🟦 Application-based
Authentication
Cryptography
Anti-Virus
Intrusion Detection
🟪 Auditing
🟥 Security Management

- Security is currently where networking was 15 years ago
- Many parts & pieces
- Complex parts
- Lack of expertise in the industry (60% vacancy with no qualified personnel)
- Lack of standards
- Attacks are growing
- Customers require security from providers

As Systems Get Complex, Attackers are Less Sophisticated…



Security Must Make Business Sense to Be Adopted



Driving Principles in Cyber Security Best Practices

- Capability Minimization
  - Allow only what is needed re: services, ports, addresses, users, etc.
  - Disallow everything else
- Partitioning and Isolation
- Defense in Depth
  - Aka “belt & suspenders”
  - Application, host and network defenses
- KISS
  - Complexity makes security harder
- General IT Hygiene
  - Backups, change control, privacy, architectures, processes, etc.
- Avoid Security by Obscurity
  - A proven BAD IDEA™

Highlights of General Issues

- Current infrastructures built on “total trust” model, which makes security very complex and difficult
- Need investment and R&D to secure infrastructures
  - Potential NRIC work items on infrastructure long-term planning for security inclusion in future architecture
- “Convergence” of network types will lead to weakened security of traditionally difficult to access networks (e.g. analog voice converges to VoIP on a data network; CDMA cellular converges to 3G on shared IP infrastructure)
- Corporate investment in security needs to be continued priority and reality

Conclusion

The FCC is just one component of a complex network of public and private partnerships dedicated to improving the security and reliability of the Nation’s telecommunications infrastructure.

Contacting The FCC

- Amal.Abdallah@fcc.gov at the FCC, International Bureau, Strategic Analysis and Negotiations Division.
- **www.fcc.gov**
- **Thank you!**