ANSI ANNUAL CONFERENCE

Homeland Security: Innovation, Collaboration, Standardization

Cyber Security (Panel VI)

The Role of Best Practices

in Protecting the Public Communications Infrastructure

Washington, D.C. – October 2003

KARL F. RAUSCHER

Director Network Reliability Office, Lucent Technologies Bell Labs
Chair FCC NRIC VI Homeland Security Physical Security Focus Group
Chair FCC NRIC V Network Reliability Best Practices Subcommittee
Vice Chair ATIS Network Reliability Steering Committee (NRSC)
Founder & President Wireless Emergency Response Team (WERT)
Chair-Elect IEEE Technical Committee on Communications Quality & Reliability (CQR)
Representative U.S. DHS National Coordinating Center (NCC) for Telecommunications, Telecom-ISAC

The Role of Best Practices in Protecting the Public Communications Infrastructure

Communications Infrastructure - 2003

- Dynamic changes in technology
- Historic economic challenges
- Fierce Competition
- Uncertain regulation

- A Critical infrastructure . . .
  - Heavily depended on by other critical infrastructures
  - With significant trends affecting its Cyber dimension
    - Custom hardware, software and protocols
      . . . to off-the-shelf systems and applications
    - Special systems built with real-time communications considerations
      . . . to standard computing platforms
    - In-house design, development and testing
      . . . to offshore outsourcing

The Role of Best Practices in Protecting the Public Communications Infrastructure

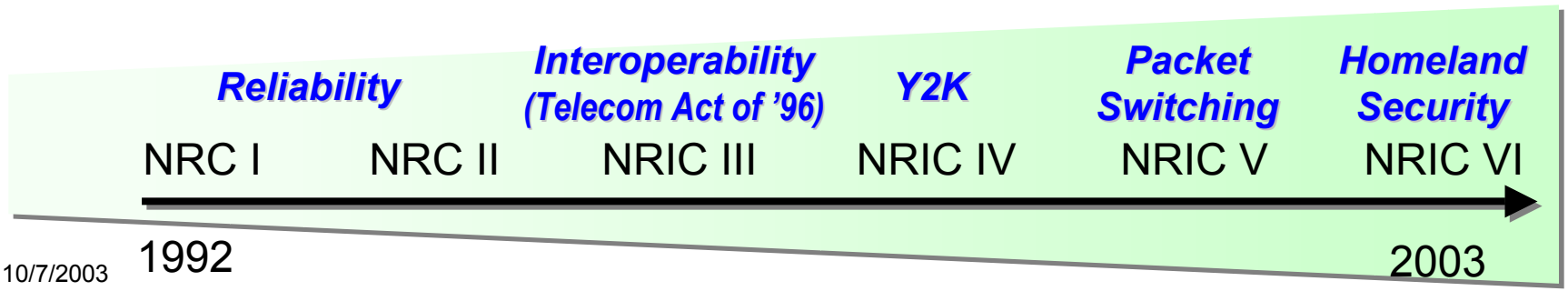
Key Fora for Communications Infrastructure

- FCC Network Reliability and Interoperability Council (NRIC)
- U.S. Department of Homeland Security National Communications System (NCS) National Coordinating Center for Telecommunications (NCC) Telecom-ISAC
- ATIS Network Reliability Steering Committee (NRSC)
- President's National Security Telecommunications Advisory Committee (NSTAC)
- QUEST Forum TL 9000
- CERT-USA
- IEEE Communications Society (International) Technical Committee on Communications Quality and Reliability (CQR)

The Role of Best Practices in Protecting the Public Communications Infrastructure

FCC NRIC History

- The Network Reliability and Interoperability Council (NRIC) VI
  - Successor to the Network Reliability Council (NRC)
    - first organized by the Federal Communications Commission (FCC) in January of 1992.
    - established following a series of major service outages
    - study the causes of service outages and to develop recommendations to reduce their number and their effects on consumers.
  - Composed of CEO-level representatives
    - service providers & network operators
    - equipment suppliers
    - state regulators, and large and small consumers (industry associations)
  - Subject to the Federal Advisory Committee Act (FACA) guidelines



The Role of Best Practices in Protecting the Public Communications Infrastructure

NRIC VI Charter - Summary

- Give telecommunications industry leaders the opportunity to provide recommendations to the FCC and to the industry that, if implemented, would under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, and cable public telecommunications networks. This includes facilitating the reliability, robustness, security, and interoperability of public telecommunications networks.

- The scope encompasses recommendations that would ensure the security and sustainability of public telecommunications networks throughout the United States;

- Ensure the availability of adequate public telecommunications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitating the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of telecommunications services

The Role of Best Practices in Protecting the Public Communications Infrastructure

Scope

- Network Types
  - wireline, wireless, satellite, cable, and the Internet
  - circuit switched, packet switched and converged technologies
- Industry Roles
  - service providers, network operators, equipment suppliers
- Security in context of Homeland Security
  - Understand “Physical” and “Cyber” to ensure 100% coverage
  - In context of Homeland Security:
    - Reliability of Services
    - Security of Networks
    - Security of Enterprises
- Threat Sources
  - terrorist activities, natural disasters, or similar types of occurrences

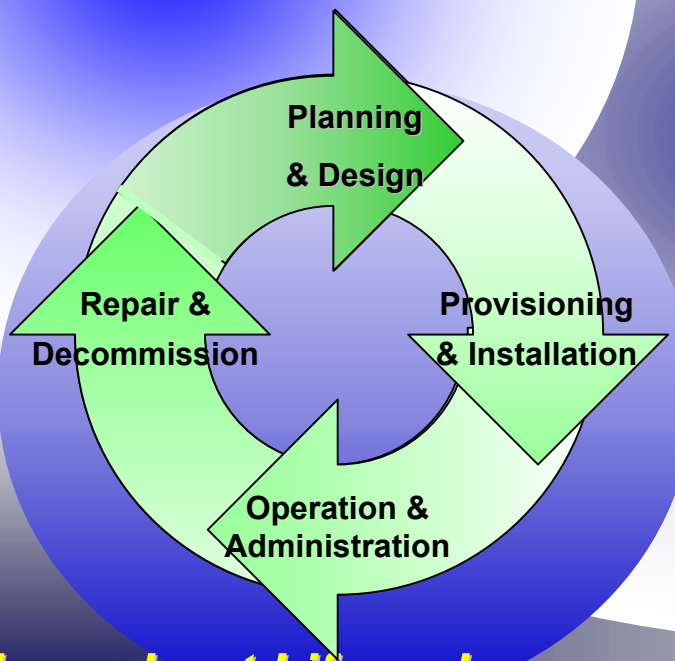
The Role of Best Practices in Protecting the Public Communications Infrastructure

Best Practices in My Company

COMMUNICATIONS INFRASTRUCTURE			
Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

Across Network Types

All Elements



Throughout Lifecycle

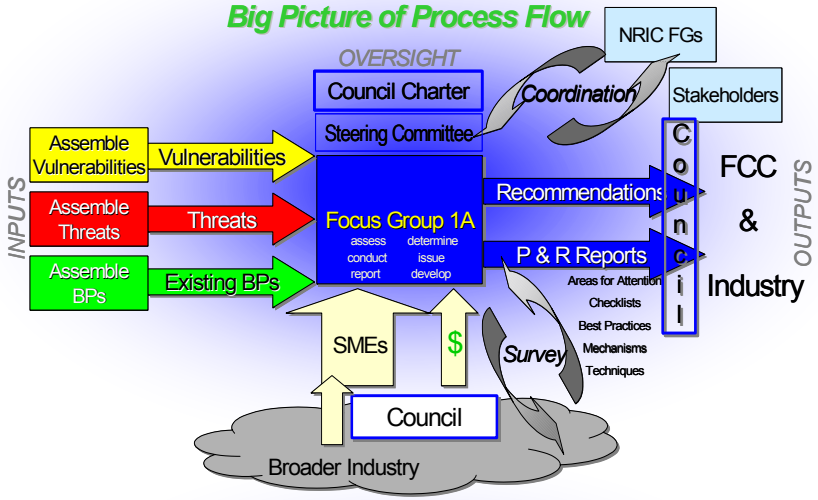
Throughout Organization Functions & Levels

The Role of Best Practices in Protecting the Public Communications Infrastructure

Characteristics of the Best Practice Development Process

Rigorous Process

Big Picture of Process Flow



Authoritative

Team Membership

Service Providers & Network Operators			
Ed Bicke		Daniel Jenkins	Intelsat
Steve Michalecki	ALLTEL	Delgie Jones Craig McQuate	Level(3) GENUITY
David Porte	AMERICAN TOWER CORPORATION	Loye Manning	NEXTEL
P.J. Aduskevicz Rick Canaday Frank Maguire	AT&T	John Morovich	PanAmSat
Jennifer Meredith	AT&T Wireless	Keith Hopkins Bob Postovit	Qwest
Ralph Whitlark Shawn Cochran	BELLSOUTH	Percy Kimbrough	SBC
Michael Clements	CABLE & WIRELESS	John Cholewa	Sprint.
Jayne McCullough Thomas Priore, Jr	Comcast.	Wayne Chiles Dick Craft Liz Geddes Roger Kochman	verizon
Scott Jones Everett Dennison	DOBSON	Craig Swenson	WORLDCOM.

Equipment & Software Suppliers	
Steve McOwen Chris Miller Art Reilly	Cisco Systems
Richard Biby	Crown Castle
Steven Warwick	HARRIS
Karl Rauscher Jim Runyon Rick Krock Ted Lach Anil Macwan	Lucent Technologies
Cathy Purvis	MOTOROLA
Mike Kennedy	NORTEL NETWORKS
Virgil Long	TIXLIC
Chao-Ming Liu	Telcordia Technologies
Fred Tompkins	UNISYS

Government & Other Entities	
Bill Klein	ATIS
Eric Guerrino Jennifer Dickerson Heather Wyson	BITS
Rick Kemper	CTIA
Ken Buckley	Federal Reserve System
George Caldwell	IBSS
Al Woods	New York Clearinghouse
Perry Fergus Larry Stark	
Hank Kluepfel	SAIC
Molly Schwarz	Schwarz Consulting
Eve Perris	Tech2000 Inc.
Tom Soroka, Jr	USTA
John L. Clarke III	

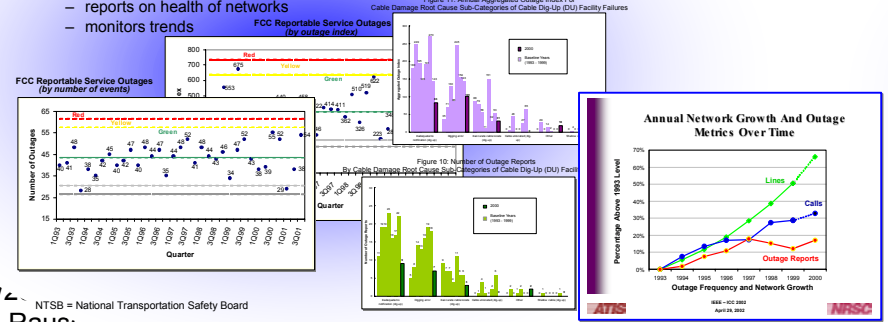
Demonstrated Effectiveness

Examples of Industry Cooperation Success

www.atis.org, then "NRSC"

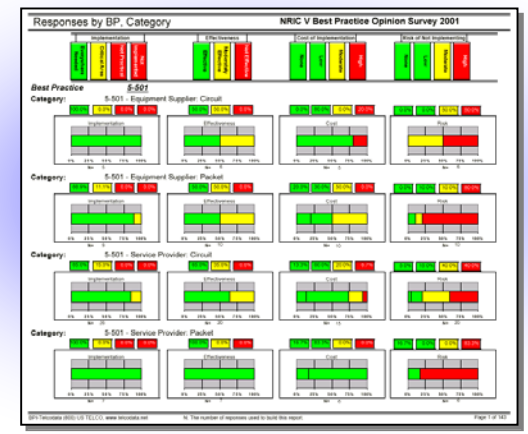
ATIS Network Reliability Steering Committee (NRSC)

- provides NTSB-like function
- reports on health of networks
- monitors trends



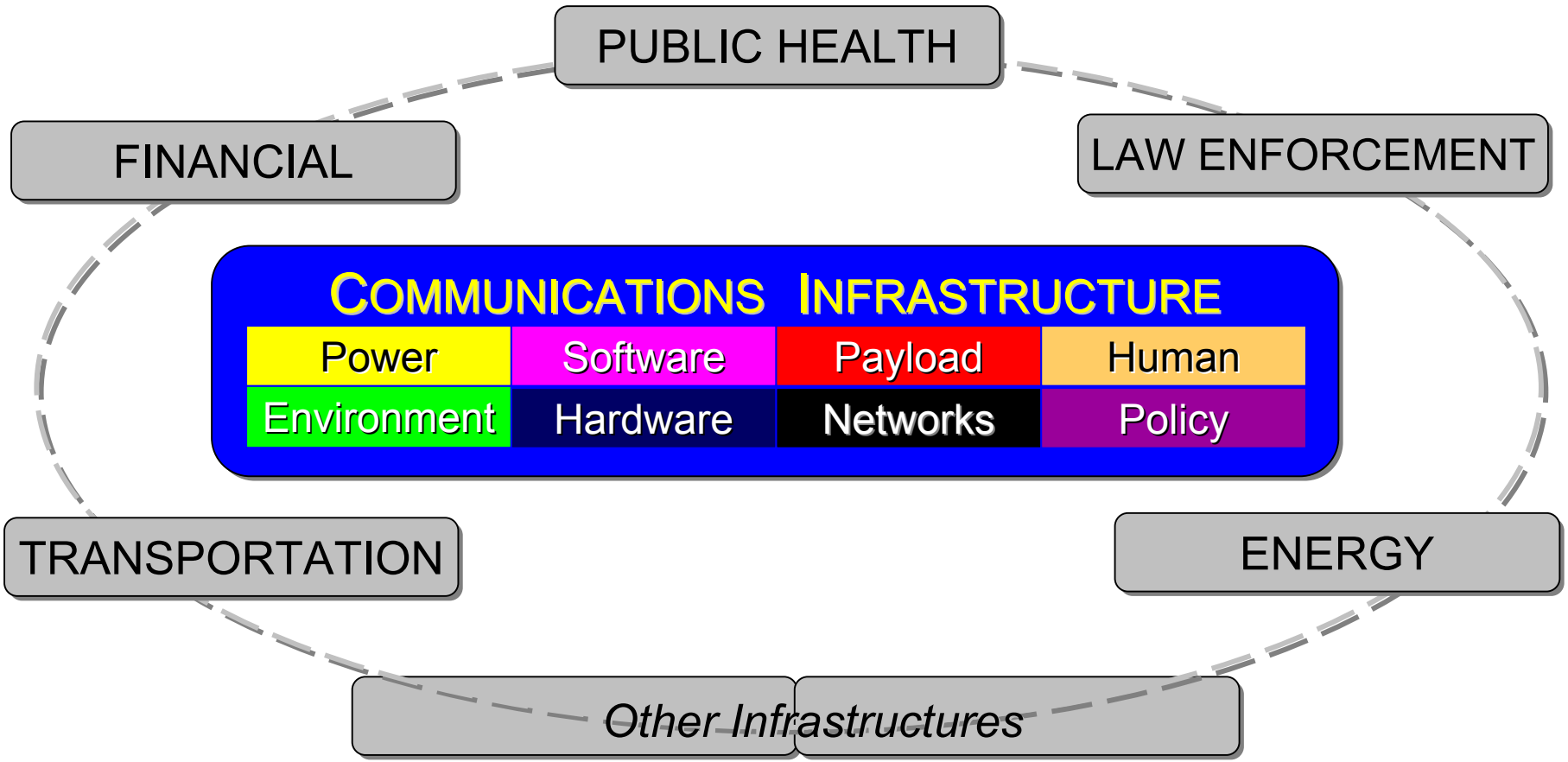
NTSB = National Transportation Safety Board

Broad Industry Support



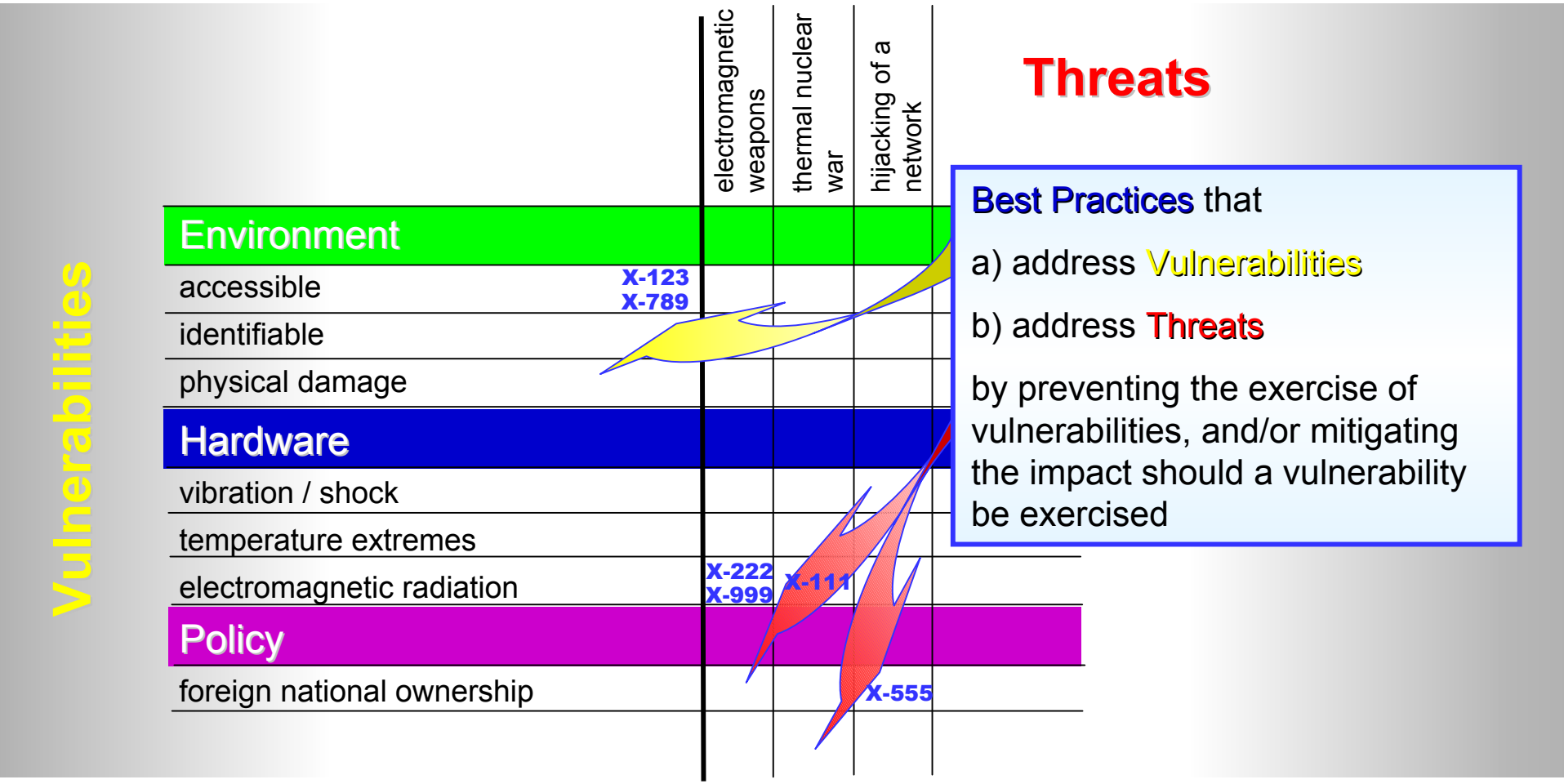
The Role of Best Practices in Protecting the Public Communications Infrastructure

Communications Infrastructure

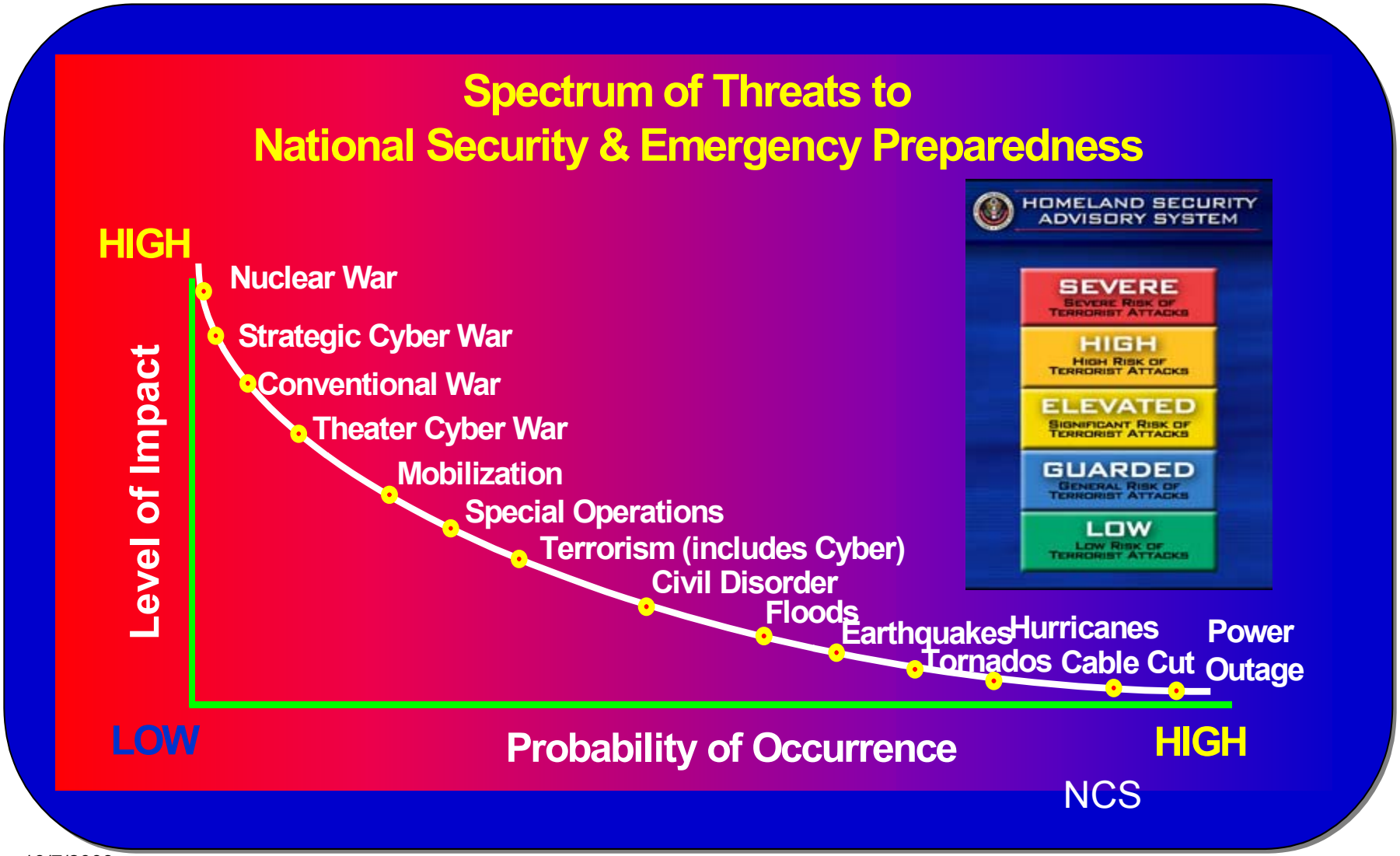


The Role of Best Practices in Protecting the Public Communications Infrastructure

Vulnerabilities – Threats - Best Practices Framework



The Role of Best Practices in Protecting the Public Communications Infrastructure

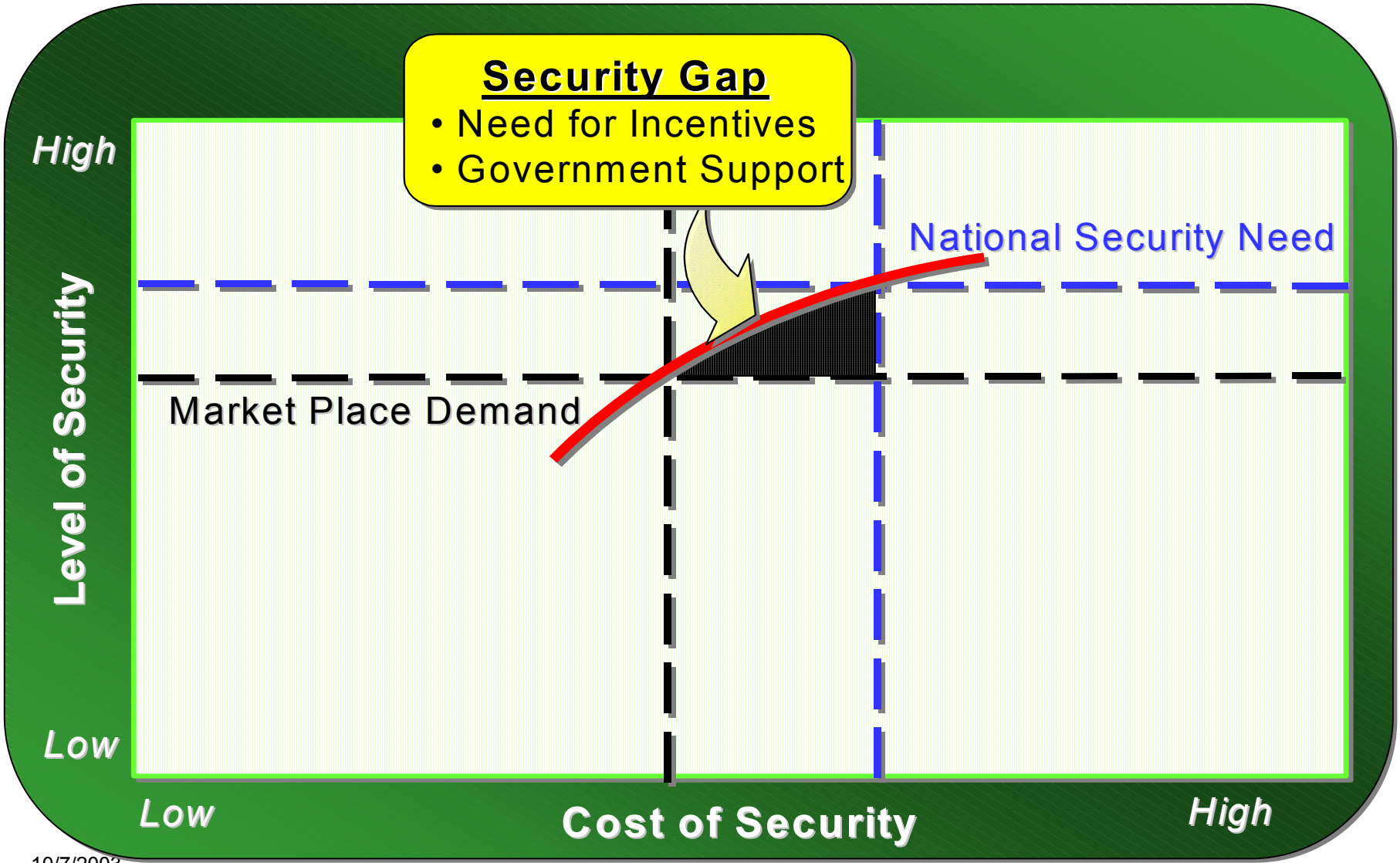


The Role of Best Practices in Protecting the Public Communications Infrastructure

Some Nuggets

- Best Practices vs. Standards vs. Regulations
- Implementation is Voluntary
- Vulnerabilities vs. Threats
- Much of investment to Cyber is reactionary
  - discipline of classical quality control principles
  - bold initiative to develop next generation of programming languages and compliers

The Role of Best Practices in Protecting the Public Communications Infrastructure



The Role of Best Practices in Protecting the Public Communications Infrastructure

Best Practices Access via Web

~ 750 Best Practices

- ~ 250 Network Reliability & Interoperability
- ~ 250 Physical
- ~ 150 Cyber Security
- ~ 50 Business Continuity
- ~ 50 Public Safety

The Role of Best Practices in Protecting the Public Communications Infrastructure

"Take Aways"

- NRIC Best Practices provide unparalleled guidance for the communications industry for
- When implemented, Best Practices are effective
- Decisions for individual Best Practices implementation should be made by experts within each company

"Secure the Homeland"

The Focus Group's deliverables are devoted to technical and policy discussions of Security; this page is devoted to the Homeland.

The Homeland is a place where we value our communications infrastructure because we value our communication.

The Homeland is a place where we value our communication because we value our words.

The Homeland is a place where we value our words because we value thoughts and beliefs.

The Homeland is a place where we value thoughts and beliefs because we value each other.

The Homeland must be Secured.

KARL F. RAUSCHER
CHAIR, NRIC VI HOMELAND SECURITY PHYSICAL SECURITY FOCUS GROUP