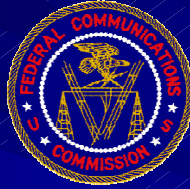


Network Security Policy: The U.S. Experience



Patricia Cooper
International Bureau
U.S. Federal Communications Commission

Network Security: The U.S. Experience

- Network Security: How we define it
- U.S. Approach: Industry Partnerships
- NRIC and MSRC
- Best Practices Recommendations
- Regulatory Observations

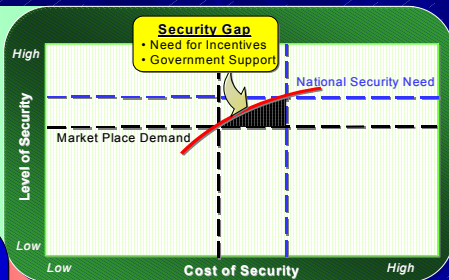
Network Security: Definitions

- Addresses the security and reliability of the physical U.S. telecommunications and media networks from natural disasters or man-made attacks
- Part of larger “Cybersecurity” Issue
 - Includes information security, privacy, data protection and law enforcement, among others

3

The Need to Address Physical Security and Reliability

- Communications Infrastructure is
 - Vast
 - Very Complex
 - Vital



- Natural Disasters Require restoration
- New Man-made Threats have emerged

4

TELECOM: Network Reliability and Interoperability Council (NRIC)

- A Federal Advisory Committee chartered by the U.S. FCC
 - Originally chartered in 1992 in the wake of major service outages
 - Re-chartered in January 2002 to focus on homeland security issues and include wireless and satellite systems
- www.nric.org

















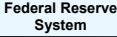



















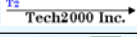

5

NRIC: Mission

- “Partner with the Federal Communications Commission, the communications industry and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices across the burgeoning telecommunications industry.” (NRIC VII)
- Accomplished through development and deployment of industry **Best Practices** to promote network reliability and interoperability
- www.nric.org

6

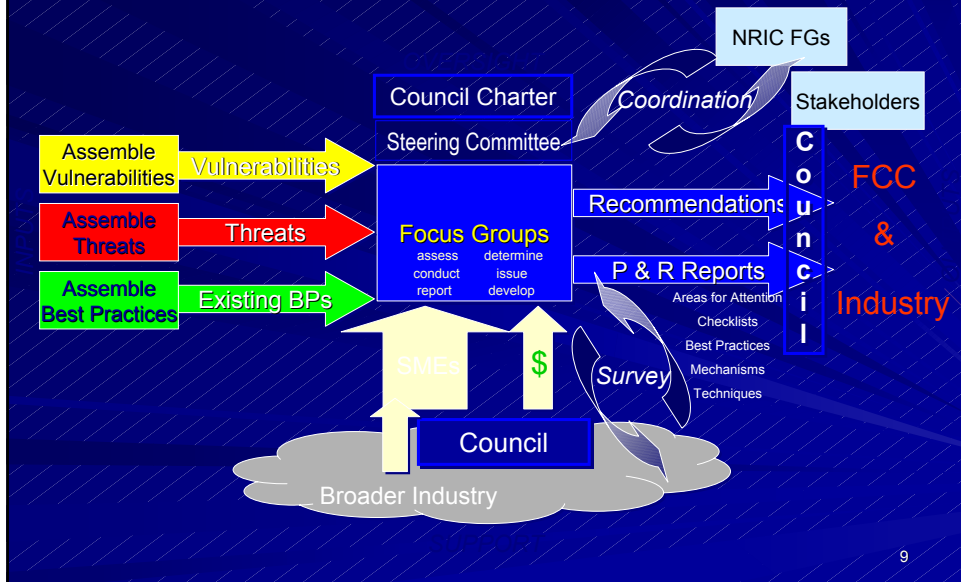
NRIC: A Partnership with Industry

Service Providers & Network Operators	Equipment & Software Suppliers	Government & Other Entities
 		
 		<p>Eric Guerrero Jennifer Dickerson Heather Wyson</p> 
 		
  		<p>Ken Buckley</p> 
 		
 		<p>New York Clearinghouse</p> 
 		
 		<p>Schwarz Consulting</p> 
 		<p>Tech2000 Inc.</p> 
		<p>John L. Clarke III</p> 

NRIC: How it works

- Partnership with Industry, Federal, State and Local Government and interest groups
- Four Focus Groups:
 - Physical Security
 - Cybersecurity
 - Business Continuity and Disaster Recovery
 - Public Safety
- Develop “Best Practices” (BPs)
 - Provide guidance on how best to protect the U.S. communications infrastructure
 - VOLUNTARY operational and technical recommendations

Big Picture: Work of NRIC



9

NRIC Best Practices: Examples

- **Sample: Physical Security Best Practice**
 - “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.” (6-P-5190)
- **Sample: Business Continuity Best Practice**
 - “Service Providers and Network Operators should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites.” (FG 1D: 6-6-1030)
- **Sample: Public Safety Best Practice**
 - “...It is particularly important to coordinate disaster exercises with other Service Providers, Public Safety Providers and vendors. It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.” (6-6-599)

10

MEDIA: Media Security and Reliability Council (MSRC)

- A Federal Advisory Committee chartered by the U.S. FCC
- Created in March 2002 to address broadcast, cable and satellite homeland security issues.
- www.mediasecurity.org

11

MSRC: Objectives

- Ensure the security and sustainability of broadcast and multichannel video programming distribution (MVPD) facilities.
- Ensure the availability of adequate transmission capability during natural disasters or man-made attacks.
- Facilitate the rapid restoration of broadcast and MVPD services in the event of significant disruptions.
- Ensure that critical communications is available to the public during and after a disaster while protecting the means to do so.

12

MSRC: Membership

- Harris Broadcast Communications
- National Association of Broadcasters
- Association of Public Television Stations
- National Public Radio
- National Cable and Telecommunications Association
- MSTV, Inc.
- Tribune Company
- NBC
- Walt Disney Company
- Univision Communications, Inc
- Belo Broadcasting
- Hearst-Argyle Television, Inc.
- Emmis Communications Corp.
- Pegasus Communications Corp
- Thirteen/WNET
- Clear Channel Communications, Inc.
- Cumulus Radio
- Radio One, Inc.
- Hispanic Broadcasting Corp
- WETA
- Sellers Broadcasting, Inc.
- Time Warner Cable
- T&T Broadband Services
- Comcast Corporation
- Cox Enterprises, Inc.
- usquehanna Communications
- Armstrong Utilities
- DirecTV, Inc.
- EchoStar Communications Corp.
- XM Satellite Radio, Inc.
- SES Americom, Inc.
- PanAmSat Corporation
- Intelsat Global Service Corporation
- VerestarAmerican Tower Corporation
- International Association of Chiefs of Police
- National Translator Association
- American Planning Association
- National Captioning Institute
- News Corp.

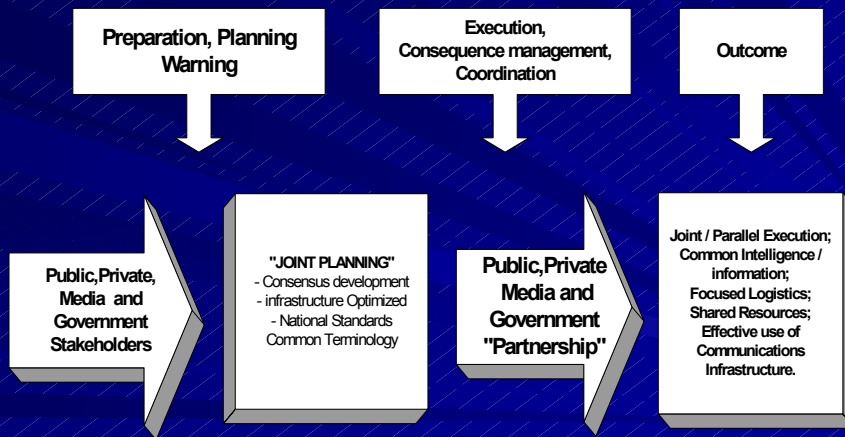
13

MSRC: How it works

- **Two Working Groups:**
 - Public Communications and Safety
 - Communications Infrastructure Security, Access and Restoration.
- **Develop Best Practices**
 - Identify strategies that ensure the operation of broadcast and MVPD facilities before, during and after a major event.
 - Provide FCC and industry with recommendations for detecting, preparing for, preventing, protecting against, responding to and recovering from terrorist threats, natural disasters or other attacks upon U.S. media infrastructure.

14

Big Picture: Work of MSRC



15

Example: MSRC Best Practices

- **Sample: Best Practices for Prevention/Communications Infrastructure Security, Access & Restoration Working Group**
 - “In order to cost-effectively gain additional geographic diversity, news networks should consider the possibility of a backup carriage plan with other non-news networks that can be exercised under government declared emergency conditions.” (Rec. 1.2.1)
- **Sample: Best Practices for Public Communications and Safety**
 - “All local media should form emergency jurisdiction / market cooperatives to assure delivery of local government emergency messages in a coordinated way to all constituencies in the community.” (Rec. 4)

16

Guiding Principles for Developing Best Practices

- “**People** Implement Best Practices”
- **Do not endorse** commercial or specific “pay for” documents, products or services
- Address **classes** of problems
- Look for solutions **that have already been implemented/tried**
- Developed by **industry consensus**
- Best Practices are verified by a **broader set** of industry members
- **Sufficient rigor and deliberation**

17

Caveats for Best Practices

- Current list of best practices are constrained by what can be implemented
- Not all best practices are appropriate for all service providers or architectural implementations
- The best practices are not intended for mandatory regulatory efforts
- **Best Practices will require *continual* refinement, additions and improvement**

18

Network Security: From the Regulators Viewpoint

- The FCC's regulatory mandate includes the security of U.S. networks
- The FCC currently addresses network security through **voluntary** standards, developed by private industry
 - Industry input improves security “best practices” recommendations
 - Broad industry participation improves compliance
- Questions for the future:
 - Ongoing questions of “who pays?”
 - Political pressure for more regulatory intervention and oversight

19

Network Security: International Cooperation

- FCC, NRIC and MSRIC increasingly are discussing network security with international counterparts
- Outreach is essential, given the global nature of networks, services and threats to security of physical communications infrastructure worldwide

20

Network Security: International Initiatives

- Europe: Formation of ENISA adds to ongoing individual network operators' security efforts
- Latin America: Organization of American States initiative on Cybersecurity includes network security component, through CITEL
- Asia: APEC drafting recommendations on cybersecurity (hacking, encryption, spam) through APEC-Tel
- ITU: Next Generation Networks Study Group under ITU-T developing standards for network security

21

CONCLUSION

- The FCC is just one component of a complex network of public and private entities, partnerships and organizations seeking to improve the security and reliability of the U.S. and global communications infrastructure.



22

Thank you!

For more information, refer to:

www.fcc.gov

