Cybersecurity Risk Management Guide for Voluntary Use of the NIST Cybersecurity Framework

Joint Meeting Committee on Critical Infrastructure and Telecommunications

July 13, 2015
New York City

Robert H. Mayer
VP Industry and State Affairs
United States Telecommunications Association

National Policy Guidance

It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. **We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.**

White House
Executive Order 13636
February 2013

We cannot hope to keep up if we adopt a prescriptive regulatory approach. We must harness the dynamism and innovation of competitive markets to fulfill our policy and develop solutions. We are therefore challenging private sector stakeholders to create a "new regulatory paradigm" of business-driven cybersecurity risk management.

FCC Chairman Tom Wheeler
American Enterprise Institute
June 12, 2014

Risk Management Roadmap

Enterprise-Level Cybersecurity Risk Management

CSRIC Cybersecurity Best Practices - March 2015

WG 4

Executive Order 13636 February 2013

NIST Cybersecurity Framework 1.0 – February 2014

Critical Infrastructure Cyber Community C³ Voluntary Program

Project Leadership

WG4 Leadership Team

- Co-Chairs: Robert Mayer, USTelecom and Brian Allen, Time Warner Cable
  - Segment Leads
    - Broadcast, Kelly Williams, NAB
    - Cable, Matt Tooley, NCTA
    - Wireless, John Marinho, CTIA
    - Wireline, Chris Boyer, AT&T
    - Satellite, Donna Bethea Murphy, Iridium
  - Feeder Group Initiatives
    - Requirements and Barriers to Implementation, Co-Leads, Harold Salters T-Mobile, Larry Clinton, Internet Security Alliance
    - Mids/Smalls – Co-Leads, Susan Joseph, Cable Labs, Jesse Ward, NTCA
    - Top Cyber Threats and Vectors - Russell Eubanks, Cox, Joe Viens, TWCable
    - Ecosystem – Shared Responsibilities, Co-Leads, Tom Soroka, USTelecom, Brian Scarpelli, TIA
    - Measurement, Co-Leads, Chris Boyer, AT&T, Chris Rosenraad, TimeWarnerCable

Advisors

- Donna Dodson, WG4 Senior Technical Advisor, NIST, Deputy Chief Cybersecurity Advisor & Division Chief for Computer Security Division
- Lisa Carnahan, NIST, Computer Scientist
- Emily Talaga, WG4 Senior Economic Advisor, FCC
- Tony Sager, Center for Internet Security

Engineering and Operational Review

- Co-Leads - Tom Soroka, USTelecom and John Marinho, CTIA
- Segment Leads Support

Drafting Team

- Co-Leads – Stacy Hartman and Paul Diamond, CenturyLink, Robert Thornberry, Alcatel/Lucent

Project Structure

BROADCASTING

There are more than 14,000 radio and 1,700 television broadcasting facilities in the United States, sending broadcasts through the air to a frequency network of transmitters.

CABLE

The cable industry is composed of approximately 7,791 cable systems that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service.

WIRELESS

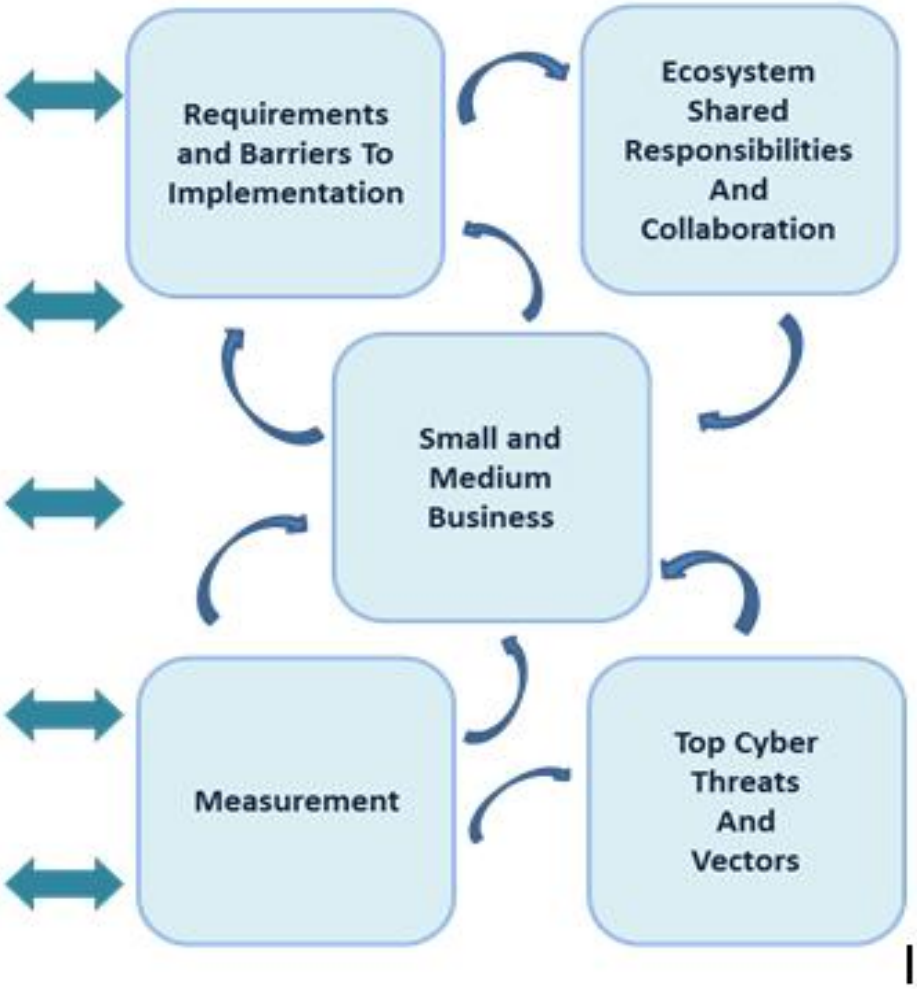
Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

WIRELINE

Over 1,000 companies offer wireline, facilities-based communications services in the United States. Wireline companies serve as the backbone of the Internet.

SATELLITE

Satellite communications systems deliver advanced data, voice, and video communications, transmitting data from one point on the Earth to another.



Project Structure and Analytics

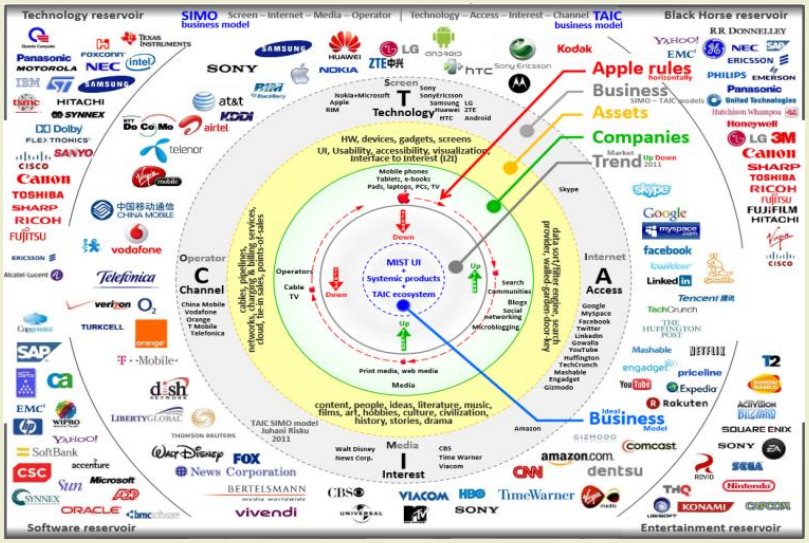
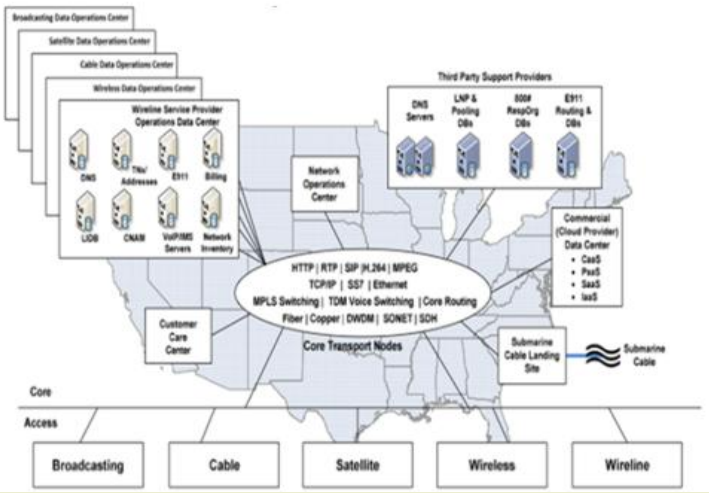
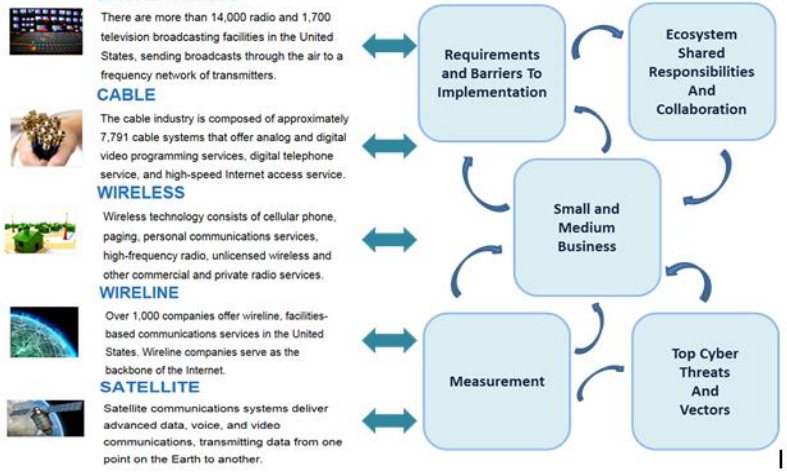


Figure 2-3 illustrates the various network components that comprise the "core network":

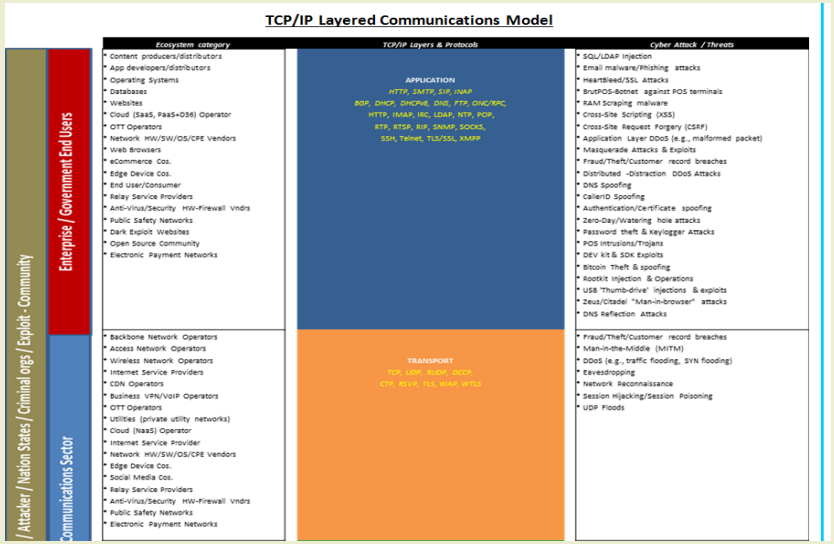


V. Appendix

Function	Category	Subcategory		Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**Operational Requirement(s):** Appropriate and adequate Operations staff may be assigned to locate, track, count, and document all critical infrastructure *network hardware, computing systems, physical machines, virtual machines, virtual and physical network circuits, staff devices, mobile devices, receivers, transmitters, antennas, optical systems, transportation systems and any system or device that has computing, storage and network connectivity functions.* * Additional levels of staff trust and training may be established for this requirement. **Technology Requirement(s):** Operations staff assigned to inventory critical infrastructure network devices and systems may need easy to operate database software and technologies that can automate, scale and report on the adding and removing of networked resources that are inventoried. This automated system should detect the presence of unauthorized hardware. * It is highly recommended that computer aided design (CAD) functions, Geographic Information (GIS) mapping functions and security functions be included and integrated into these inventory database technologies. * It is highly recommended that access to this critical network inventory is extremely limited to those with a need-to-know basis. **Barriers:** When professional staff is allocated/assigned to this task, it may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust should be established and additional levels of training can take place. Database software and hardware systems may cause an additional CAPEX and OPEX cost. It is at the discretion of the technical management and staff to determine if existing hardware resources can be shared/used or if new	· **CCS CSC 1** · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **COBIT 5** BAI09.01, BAI09.02 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8

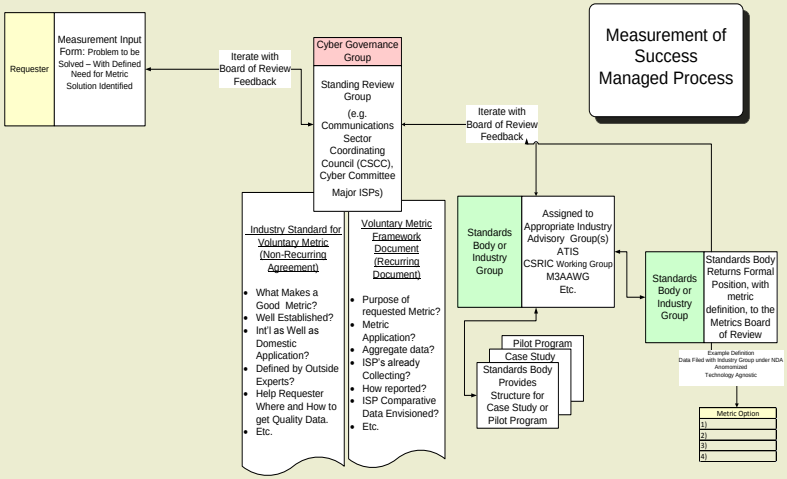


Project Structure and Analytics (Continued)



Communications Sector - Ecosystem Dependencies

Ecosystem Dependencies	Comm Sector Owners / Operators: Access Network Operator (Satellite, FTTH, Cable, DSL)	Backbone Network Operator (Fiber, Satellite, Wireless)	Broadcast	Internet Service Provider	Wireless Network Operator
App Producer/ Distributor	X	X	X	X	X
Anti-Virus/Security HW-Firewall Vendors	X	X	X	X	X
CDN Operator	X				
Cloud (XaaS) Operator		X			
Content Producer/ Distributor			X	X	X
End User /Consumer /Enterprise	X	X		X	X
Federal/State/Local Regulators	X	X	X	X	X
Government Information Sharing Bodies	X	X	X	X	X
International Svce Providers/ Content Producers	X	X		X	
Internet Service Infrastructure/ Clearinghouse	X	X		X	X
Network HW /SW /OS /CPE Vendors	X	X	X	X	X
Open Source Community	X			X	X
OTT Service Provider	X				
Relay Service Providers	X				
Research Institutions	X	X	X	X	X
Technical Standards Bodies	X	X	X	X	X
Subscriber Devices	X			X	X
Web Browsers	X			X	X



RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Best Practices	Microsoft	Tips for creating strong passwords	http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password	Provides tips for creating and maintaining strong passwords.
Best Practices	NIST	Small Business Information Security: The Fundamentals	http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf	This report assists small business management to understand how to provide basic security for their information, systems, and networks.
Best Practices	Pennsylvania Public Utility Commission	Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities	http://www.puc.pa.gov/general/pdf/Cybersecurity_Best_Practices_Booklet.pdf	The guide outlines red flags to look for and ways to prevent identity or property theft; how to manage vendors and contractors who may have access to a company's data; what to know about anti-virus software, firewalls and network infrastructure; how to protect physical assets, such as a computer in a remote location or a misplaced employee device; how to respond to a cyber-attack and preserve forensic information after the fact; and how to report incidents.
Network Protection Tool	Open Source	Network Mapper (Nmap)	http://nmap.org/	Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and

Three Macro-Level Assurances

As evidence of the Communication's Sector's commitment to enhance cybersecurity risk management capabilities across the sector and the broader ecosystem, and to promote the use of the NIST CSF, WG4 recommended the following three new voluntary mechanisms to provide the appropriate macro-level assurances.

I. **FCC initiated confidential company-specific meetings**, or similar communication formats to convey their risk management practices. The meetings would be covered by protections afforded under the Protected Critical Infrastructure Information (PCII) administered by the Department of Homeland Security (DHS) or a "legally sustainable equivalent";

II. **A new component of the Communications Sector Annual Report that focuses on segment-specific cybersecurity risk management,** highlighting efforts to manage cybersecurity risks to the core critical infrastructure; and

III. **Active and dedicated participation in DHS' Critical Infrastructure Cyber Community C³ Voluntary Program,** to help industry increase cybersecurity risk management awareness and use of the Framework.

Next Steps

- Execute voluntary mechanisms designed to give the FCC and the public assurance that communications providers are taking the necessary steps to manage cybersecurity risk.
- Participate in framework outreach and education efforts through DHS C-Cubed Program and trade association initiatives.
- CSCC organizing sector Framework Implementation Initiative to provide practical guidance and tools on use of the Framework or alternative risk management construct and to share best practices and lessons learned.
- Continue dialogue with federal and state government partners and regulators to promote risk management initiatives that foster collaboration and avoid duplication of efforts.