Cybersecurity Risk Management and Best Practices (WG 4)

Cybersecurity Framework for the Communications Sector

Final Report Presentation

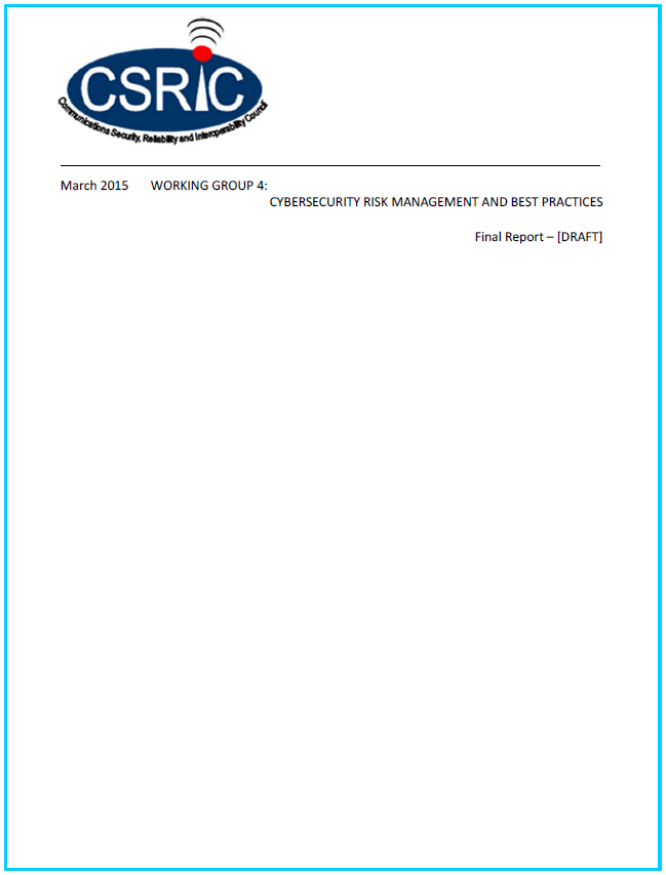
March 18, 2015

Co-Chairs:
Robert Mayer, USTelecom
Brian Allen, Time Warner Cable

CSRIC
Communications Security, Reliability and Interoperability Council

Agenda

- Introduction
- Policy Guidance
- WG4 Leadership Team and Members
- WG 4 Charge
- Report Organization
- New Voluntary Mechanisms
- Industry Guidance and Resources
- CSRIC Recommendations
- Appendix: Segment Subgroup Sample Analyses
- Questions/Discussion



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 12, 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

WG 4 Leadership Team

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

WG4 Team Members

Robert Mayer (Co-Chair)
Brian Allen (Co-Chair)
Donna Dodson (Sr Tech Advisor)
Emily Talaga (Sr Economic Advisor)
Vern Mosley (FCC Liaison)
Adrienne Abbott
Anthony Acosta
Michael Alagna
Carl Anderson
Nadya Bartol
James Bean
Chris Boyer
Chuck Brownawell
Lois Burns
Ingrid Caples
Joel Capps
Lisa Carnahan
Dan Cashman
Nneka Chiazor
Larry Clinton
Edward Czarnecki
Kate Dean
Paul Diamond
Martin Dolly
Tanner Doucet
Seton Droppers
Victor Einfeldt
Russell Eubanks
Paul Ferguson
Inette Furey
Andrew Gallo
Chris Garner
Michael Geller
My K. Gomi
Jessica Gulick
Stacy Hartman
Mary Haynes
Chris Homer
Charles Hudson, Jr
Wink Infinger
Chris Jeppson
Susan Joseph
Franck Journoud
Merike Kaeo
Kevin Kastor
John Kelly
Danielle Kriz
Rick Krock
Jeremy Larson
Greg Lucak
Ethan Lucarelli
Daniel Madsen
John Marinho
Heath E. McGinnis
Donna Bethea Murphy
Paul Nguyen
Jorge Nieves
Michael O'Reirdan
Martin Pitson
Joel Rademacher
J. Bradford Ramsay
Alan Rinker
Chris Roosenraad
Tony Sager
Harold Salters
Brian Scarpelli
Karl Schimmeck
J. J. Shaw
Ray Singh
Tom Soroka
Craig Spiezle
Matt Starr
Bill Taub
Robert Thornberry
Sheila Tipton
Matt Tooley
Bill Trelease
Colin Troha
S. Rao Vasireddy
Joe Viens
Christian Vogler
Jesse Ward
Errol Weiss
Kathy Whitbeck
Jack Whitsitt
Kelly Williams
Shawn Wilson
Pamela A. Witmer
Shinichi Yokohama

Key Elements of WG4 Charge

- Develop voluntary mechanisms which give the FCC and the public assurance that communications providers are taking the necessary steps to manage cybersecurity risks across the enterprise;
- Such assurances:
  - (1) can be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., not one-size-fits-all),
  - (2) are based on meaningful indicators of successful (and unsuccessful) cyber risk management (i.e., outcome-based indicators as opposed to process metrics), and
  - (3) allow for meaningful assessments both internally (e.g., CSO and senior corporate management) and externally (e.g., business partners).
- Demonstrate how communications providers can reduce cybersecurity risks through the application of the NIST Cybersecurity Framework or an equivalent construct**.**
- Develop implementation guidance to help communications providers use and adapt the Cybersecurity Framework developed last year by the National Institute of Standards and Technology (NIST).

Report Organization

TABLE of CONTENTS

- Report organized around the key elements in the WG4 Charge
- Includes Communications Sector Implementation Guidance
- Contains Summary Report with stand-alone Segment and Feeder Subgroup Appendices

Report Flow

Segment/Feeder Subgroup Findings

Conclusions drawn from those findings

Actionable recommendations to the FCC

Voluntary Mechanisms

1. FCC-initiated confidential company-specific meetings to include DHS as our Sector-Specific Agency (SSA):

- Companies that agree to participate would discuss efforts by the organizations to develop risk management practices consistent with the NIST Cybersecurity Framework or equivalent constructs.
- Companies would share information regarding cyber threats or attacks on their critical infrastructure, and the organizations' effort to respond or recover from such threats or attacks.
- Companies that choose to participate in this program would be afforded the protections that are given by the federal government to critical infrastructure owners and operators under the PCII program or a legally sustainable equivalent.

"This voluntary mechanism represents a new level of industry commitment intended to promote additional transparency, visibility, and dialogue with appropriate government partners and our regulator in the area of cybersecurity risk management."

CSRIC IV Working Group 4 Final Report Executive Summary

Voluntary Mechanisms

2. Expanded Sector Annual Report:

- The Sector recognizes that the increasing frequency, sophistication, and destructive nature of cyber-attacks spurs concerns about what companies are doing to manage their cybersecurity risks.
- The Measurement subgroup recommends that the Communications Sector Coordinating Council (CSCC), include information on the cybersecurity of critical communications network infrastructure in future drafts of the Sector Annual Report starting in 2015.
- The SAR would then be provided to DHS, which is the communications sector's SSA, and the Government Coordinating Council (GCC), which includes the FCC.

"This new voluntary mechanism reflects a material enhancement to the existing SAR because it would provide greater insight into the threats posed to the sector, and the actions taken to ensure continued availability of the core network infrastructure and the critical services that depend on its availability and integrity."

CSRIC IV Working Group 4 Final Report
Executive Summary

Voluntary Mechanisms

3. Active Participation in DHS C³Outreach and Education:

- DHS created the Critical Infrastructure Cyber Community C³ Voluntary Program in response to a directive contained in Executive Order 13636. The Program emphasizes three C's:
  - *Converging* critical infrastructure community resources to support cybersecurity risk management and resilience through use of the Framework;
  - *Connecting* critical infrastructure stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement, and awareness; and
  - *Coordinating* critical infrastructure cross sector efforts to maximize national cybersecurity resilience.
- The Communications Sector will develop a series of webinars and other reference materials to advance the use of the Framework through the implementation guidance contained in this report and from other sources.

"The goal is to increase awareness by sector enterprises, guide their use of the NIST CSF and explain the innovative processes, solutions, and lessons learned from the communication sector's leaders in using the Framework."

CSRIC IV Working Group 4 Final Report
Executive Summary

Comm Sector Implementation Guidance and Resources

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

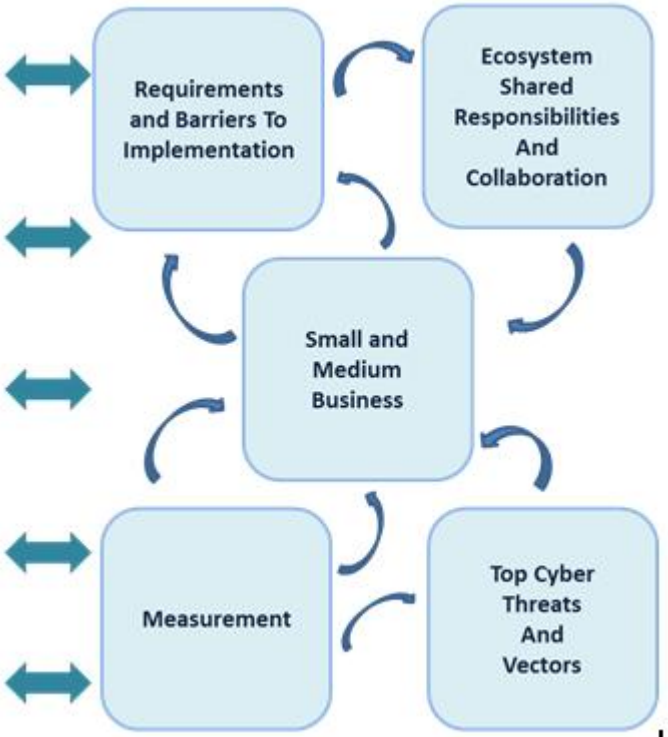
Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

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.



Implementation Guidance and Resources

Governance:

- The NIST Framework emphasizes the importance of taking a holistic approach to cybersecurity, viewing it as an enterprise-wide, strategic risk management matter, rather than as a narrow information technology (IT) or network management domain.

- For many companies, establishment of a dedicated cross-enterprise cybersecurity risk governance function can facilitate this key objective. Such a governance authority should be sufficiently representative of the organization to achieve the following:

  - Identify potential risks and a variety of risk tolerance perspectives;
  - Apply independence and authority to risk management activities;
  - Ensure transparency through the risk decision making and implementation process;
  - Define and communicate the enterprise's risk tolerance; and
  - Continually adapt and assess cybersecurity risk management goals and objectives.

"While the specific structure and operational practices of these governing bodies can and will vary among individual companies, the foundational principle is that every company should treat cybersecurity as a key component of overall enterprise risk management."

CSRIC IV Working Group 4 Final Report
Executive Summary

Implementation Guidance and Resources

In addition to the segment-specific guidance provided to broadcast, cable, satellite, wireless and wireline companies through the industry segment subgroup reports, WG4 also developed cyber risk management recommendations that apply to the sector across-the-board.

Companies are urged to:

- Review the WG4 report and use its analytical process to adapt the NIST Cybersecurity Framework approach to cybersecurity risk management to their own operations and networks;
- Distribute the NIST Cybersecurity Framework and appropriate components of the WG 4 report to company officers and personnel whose duties encompass cybersecurity management and operations;
- Ensure that operators and vendors in every layer of the TCP/IP model conduct their operations with cybersecurity diligence, to prevent and respond to attacks on their networks and operational support systems; and
- Recognize that threat knowledge is power and consider adopting a threat intelligence handling model to enhance protection of critical infrastructure. This includes sharing more detailed threat intelligence information with trusted stakeholders to improve information gathering for use in threat analyses and cyber risk management decision-making.

Comm Sector Implementation Guidance and Resources

REQUIREMENTS AND BARRIERS

CYBER ECOSYSTEM AND DEPENDENCIES

MEASUREMENT

SMALL AND MEDIUM BUSINESS

TOP CYBER THREATS AND VECTORS

Implementation Guidance and Resources

9.6 Requirements and Barriers to Implementation

- Identifies key financial, technical, legal/policy, and operational barriers for 22 CSF Categories based on Segment and SMB feedback.

1) Identify Function

Relevant Categories:	Primary Barrier:
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.	**Financial:** Barriers are dependent on the size of an organization, and costs are not linear. Marginal cost for improving Tier position is often exponential. Nonetheless, enterprises should use the NIST framework's Tier definitions to determine their current posture, and where they want to be. (FINANCIAL)

4) Respond Function

Relevant Categories:	Primary Barrier:
Response Planning (RS.RP): Response process and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**Financial:** Additional CAPEX and OPEX cost to procuring BC and DR technologies and systems and training staff to recover systems and data, in order to return the organization back to normal business operations.

Implementation Guidance and Resources

9.6 Requirements and Barriers to Implementation

- Over 100 pages outline sector-specific operational and technical resources needed to implement NIST CSF for all 98 Sub-Categories.

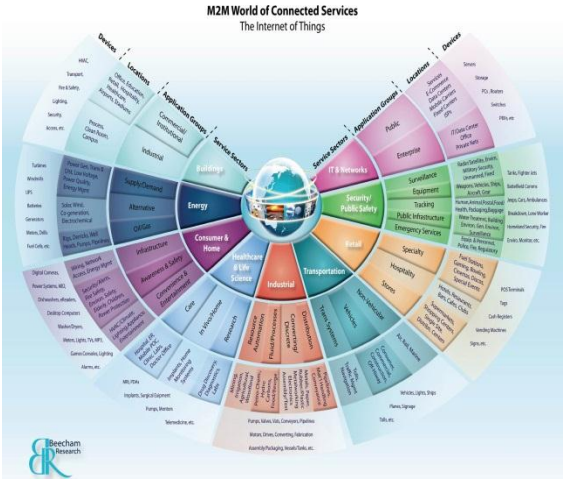
V. Appendix

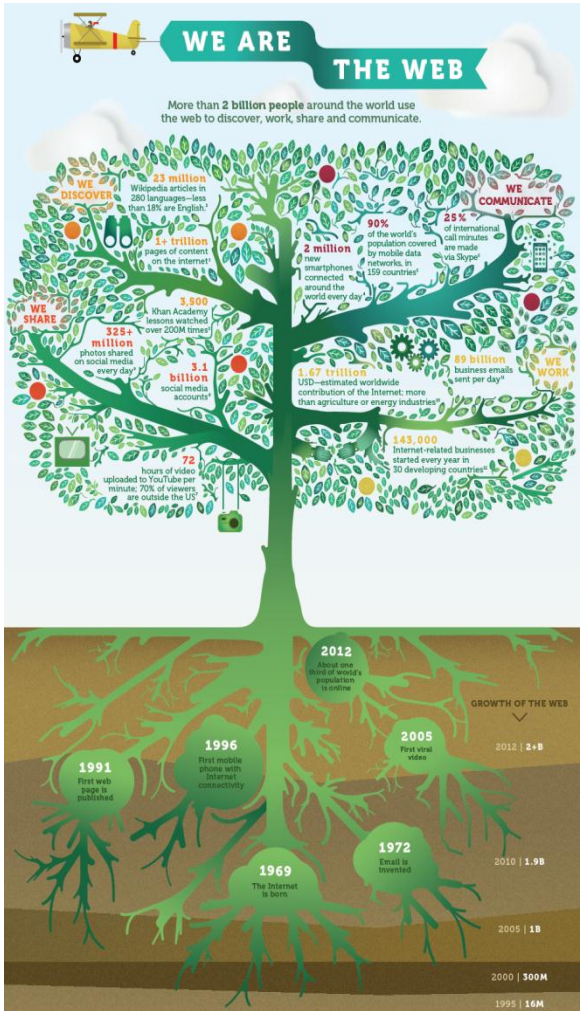
Function	Category	Subcategory		Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives 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

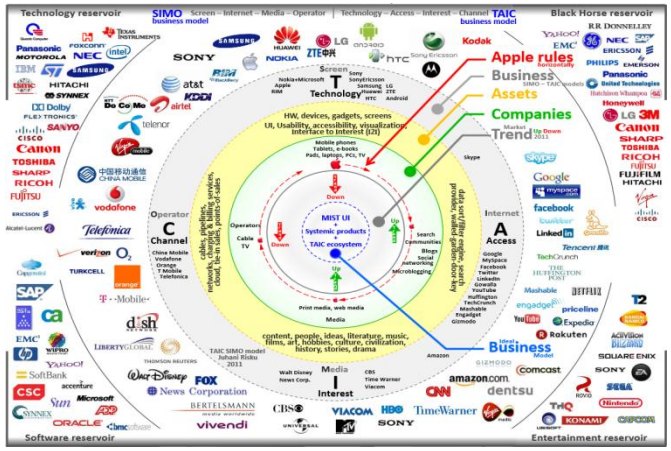
Implementation Guidance and Resources

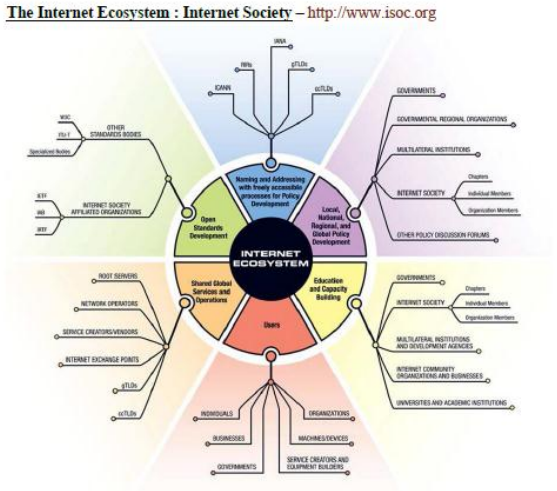
9.7 Cyber Ecosystem and Dependencies

- Multiple depictions of the Internet and comm sector ecosystem, for example:









Cyber Ecosystem Players

User/ Device	Device Provider	Provider Edge	Core	Infrastructure Provider	Application /Content
Mobility UE	O/S	Internet Control Plane (DNS/BGP/TCP/IP)	Internet Control Plane (DNS/BGP/TCP/IP)	Internet Control Plane (DNS/BGP/TCP/IP)	OTT Comms
CPE	Embedded Systems	Macro Wireless	Public Peering	DNS & IP Registrars | CAs	Social Networks
Provider-mgd Gateway	OEM	WiFi	Private Peering	Cloud	Video
M2M/IoT	AV/IDS/MDM	Broadband	Private Networks	Hosting	Applications
Corporations		High-Speed Access	Mobility EPC	CDN	
		Satellite		MSS	

Standards/Policies/Practices (e.g., IETF)

Physical Security

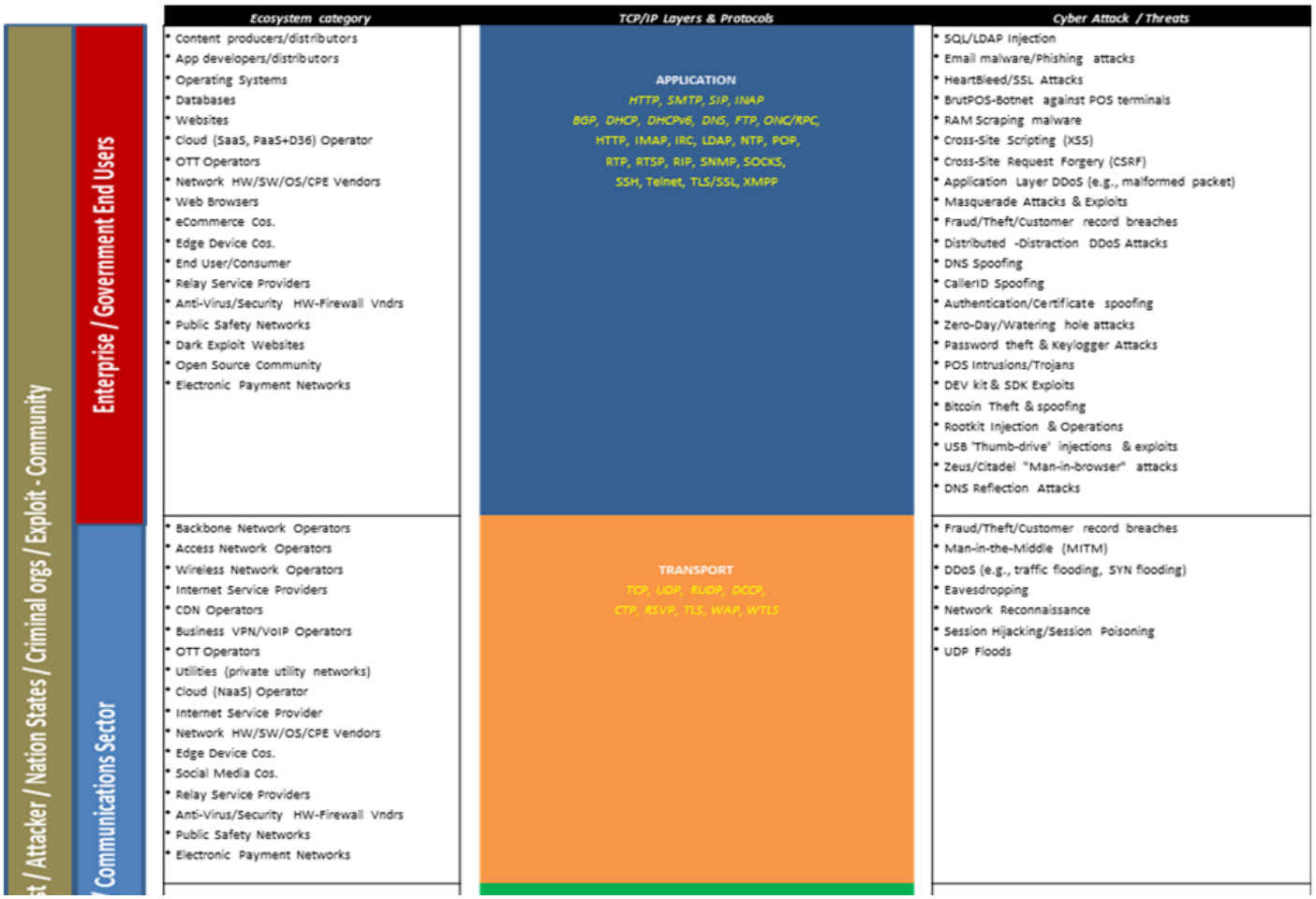
Malicious Actors

Implementation Guidance and Resources

9.7 Cyber Ecosystem and Dependencies

- Common known attacks and vectors across the Internet stack.

Ecosystem to TCP/IP Layers to Cyber Attack Mapping



Implementation Guidance and Resources

9.7 Cyber Ecosystem and Dependencies

- Identifies major Comm sector ecosystem dependencies:

Communications Sector - Ecosystem Dependencies

	Comm Sector Owners / Operators				
Ecosytem Dependencies	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

Implementation Guidance and Resources

9.7 Cyber Ecosystem and Dependencies

- Includes textual descriptions for 27 Internet and Comm sector ecosystem stakeholders.

B. APPENDIX – B Textual Descriptions of the Internet and Communications Ecosystem Categories

The categories described below are the various categories that the Ecosystem Feeder Group has identified. Each of these categories serves a specific and unique function within our Internet and communications experiences.

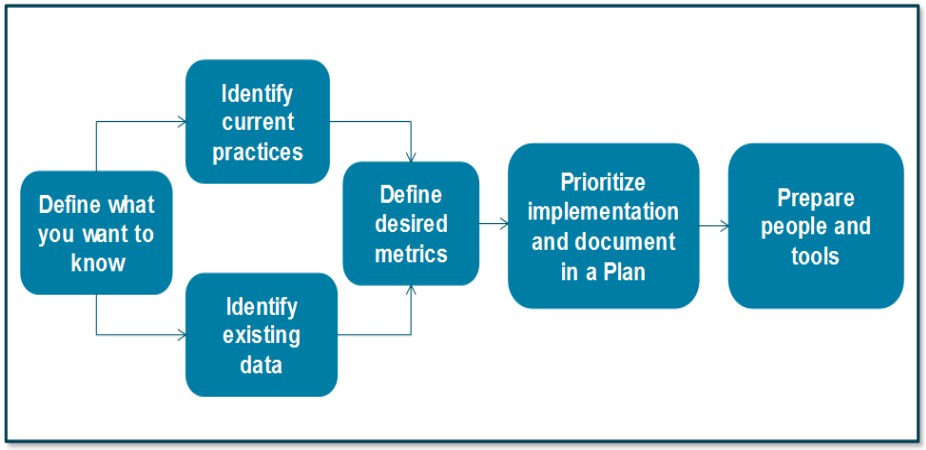
1) Backbone Network Operators

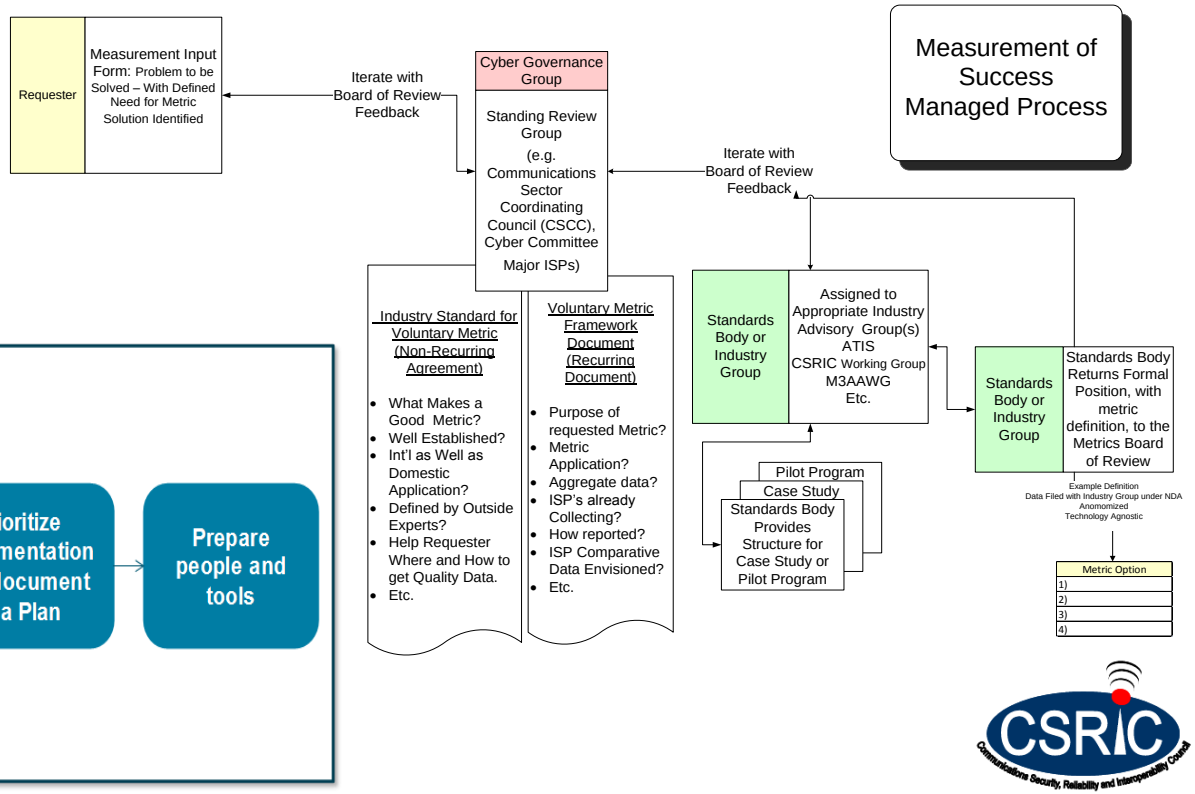
Backbone operators combine high speed transport services, such as DWDM wavelengths and/or SONET circuits, with a set of high capacity routers to create IP and MPLS networks that cover broad geographic regions. These regions can be national or international in scope. The Backbone network operators connect with other backbone and regional providers over public and private peerings to provide global Internet connectivity. The services provided by backbone operators include high speed business Internet service to Enterprises and to other Internet Service Providers. They also provide packet transport services based on IP and MPLS. Service providers such as Level 3, AT&T, and CenturyLink provide backbone network operations. Backbone Network operators typically also provide additional services on top of the backbone networks.

Implementation Guidance and Resources

9.8 Measurement

- Identifies internal process flow to create or update measures.
- Identifies process flow to review requests for additional measures.





Implementation Guidance and Resources

9.9 Small and Medium Business

- Identifies **what** an SMB needs to protect, **who** has responsibility for a given task, and **how** an SMB can protect its core network and critical infrastructure.
- Use cases from Broadcast and Cable/Wireless/Wireline segments to illustrate steps taken by SMBs in using the NIST CSF.
- Identifies highest priority NIST CSF subcategories for SMBs, for example:

Priority Practices

NIST Framework Subcategory	SMB Question
ID.AM-1: Physical devices and systems within the organization are inventoried	What
ID.AM-2: Software platforms and applications within the organization are inventoried	What
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	What
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Who
ID.GV-4: Governance and risk management processes address cybersecurity risks	What/ How

NIST Framework Subcategory	SMB Question
PR.IP-4: Backups of information are conducted, maintained and tested periodically	How
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	What
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	How
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	How
PR.PT-4: Communications and control networks are protected	How

Implementation Guidance and Resources

9.9 Small and Medium Business

- Identifies extensive list of tools, templates, reports, websites, etc., that can assist SMBs with their cybersecurity efforts, for example:

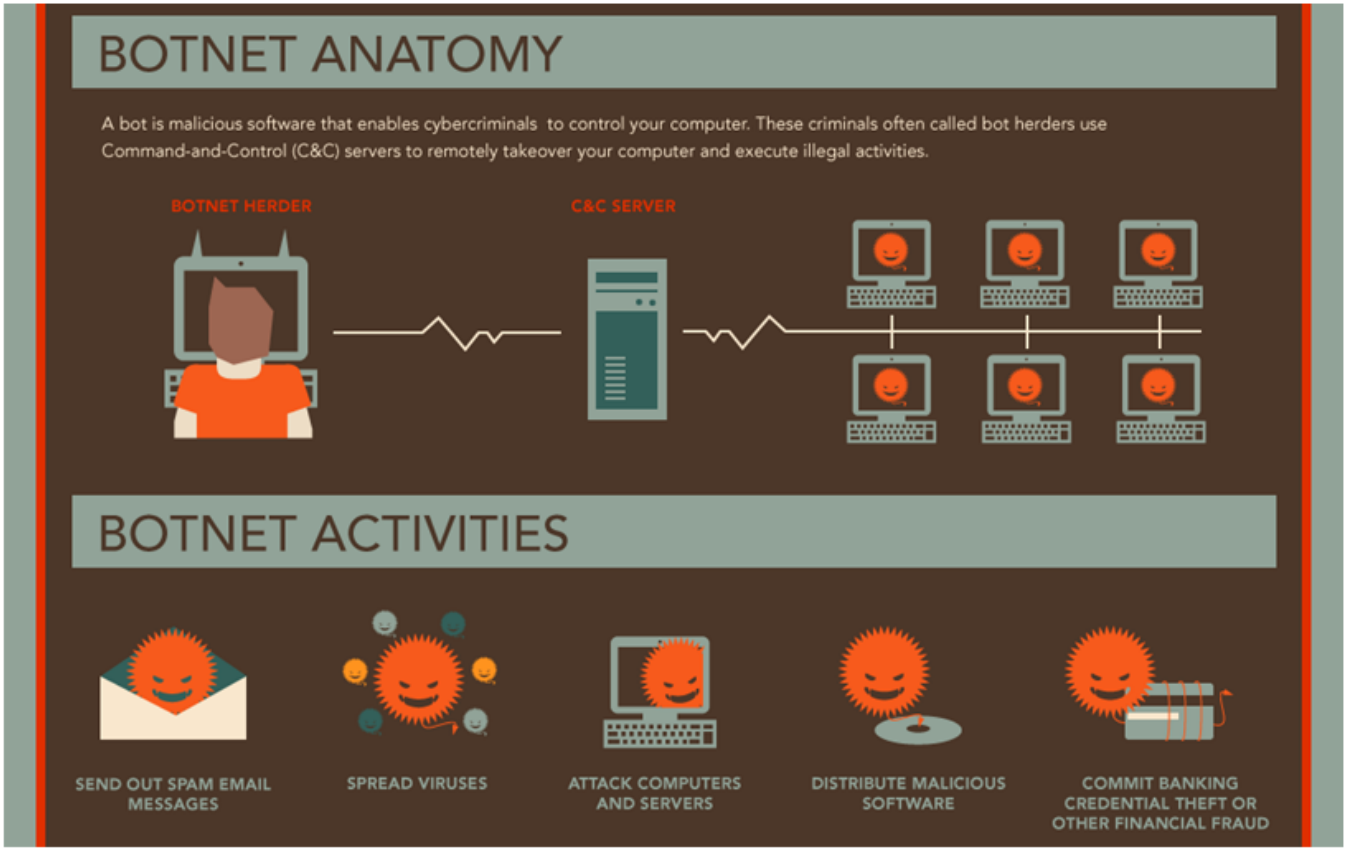
RESOURCE TYPE	SOURCE	TITLE	LINK	DESCRIPTION
Best Practices	Microsoft	Tips for creating strong passwords	http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password	Provides tips for creating and maintaining strong passwords.
Best Practices	NIST	Small Business Information Security: 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

Implementation Guidance and Resources

9.10 Top Cyber Threats and Vectors

- Identifies anatomies of typical attacks, for example:

The anatomy of a typical botnet and its activity is depicted in the graphic below:



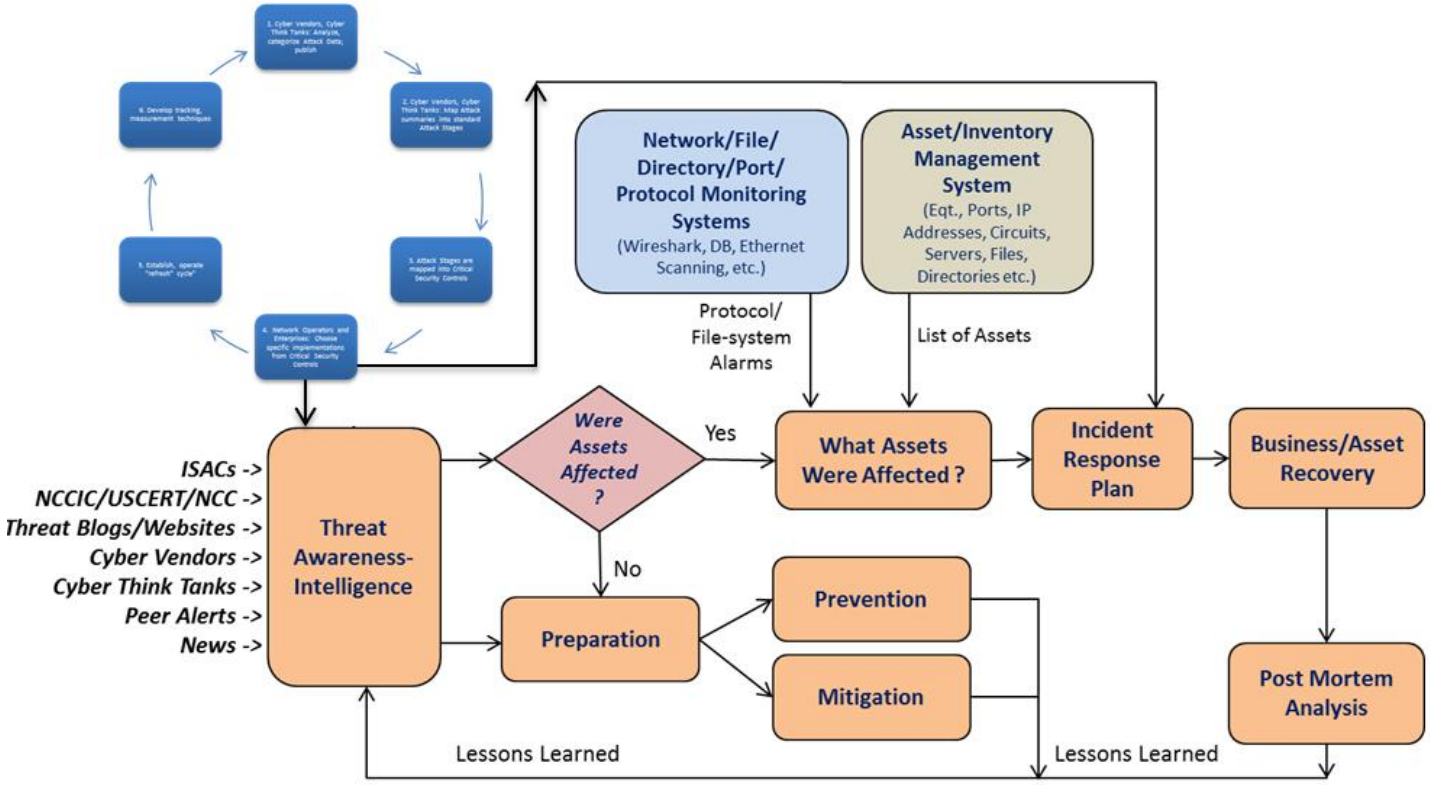
Source: Check Point Software Technologies

Implementation Guidance and Resources

9.10 Top Cyber Threats and Vectors

- Identifies an illustrative threat intelligence/information sharing process to aid an organization with making decisions and taking appropriate action:

Illustrative Threat Intelligence / Information Sharing Process Model:



Key Recommendations for FCC Consideration

The following recommendations are consistent with the Federal Advisory Committee Act (FACA) rules under which CSRIC operates. These recommendations were developed with the intention of working with the FCC and other U.S. government agencies to enhance cybersecurity risk management competencies and to make useful resources available to enterprises across the broad communications sector.

- The FCC should promote the voluntary use of the NIST CSF amongst all communications sector members, large and small, as well as across other critical infrastructure sectors that are interdependent with the communications sector.

- The FCC should encourage the dissemination of the NIST Framework and the WG 4 report to appropriate communication sector member organizations, and in particular, to management and staff with cybersecurity management and operational responsibilities.

- The FCC should work to coordinate and rationalize Framework related federal/state government initiatives to ensure efficient use of critical and scarce cybersecurity resources.

Key Recommendations for FCC Consideration

- The FCC should leverage the resources and capabilities of the three primary communications sector organizations (i.e. NSTAC, CSCC/GCC, Comm-ISAC) to promote voluntary participation in risk management initiatives across all communications segments and providers.

- The FCC should promote the sustained voluntary collaboration and facilitate the sharing of cybersecurity threat information. This can be accomplished by working with the communications sector members and other relevant agents of the U.S. government to identify and mitigate technical, operational, financial and legal barriers to cyber information sharing.

- The FCC should further evolve the understanding of the changing threat landscape, sector ecosystem dependencies, and harmonization with previous CSRIC best practices and the NIST CSF.

Key Recommendations for FCC Consideration

- The FCC should promote an industry threat intelligence handling model (referenced in this report), or an equivalent construct by organizations intending to use threat intelligence to maintain cybersecurity, protect critical infrastructure and protect critical data from rapidly evolving cyber threats.

- The FCC should encourage communications sector members to share relevant threat intelligence information (consistent with applicable law) with appropriate stakeholders, thus enabling more efficient and scalable threat information gathering for use in threat analyses and cyber risk management decision-making.

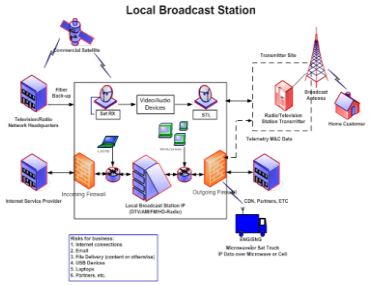
- The FCC should further explore the considerations and accommodations that are required for Small and Medium business (SMB) to implement the NIST Cybersecurity Framework and provide macro-level assurances to the FCC and the public.

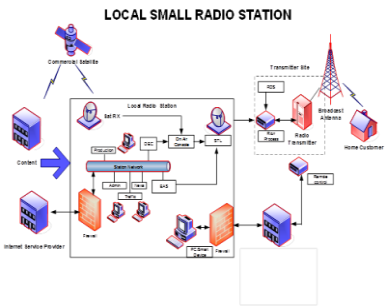
- The FCC should adopt availability of the critical communications infrastructure as the meaningful indicator of cybersecurity risk management.

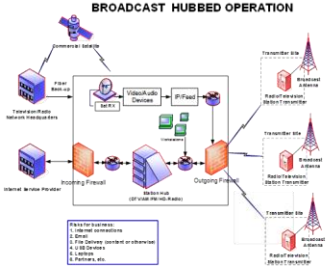
Implementation Guidance and Resources

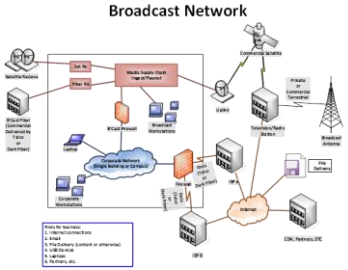
9.1 Broadcast Segment report:

- Includes an analysis of the four primary types of broadcast operations (i.e., small radio station, local TV broadcast station, station hub and broadcast network) with their risks.
- Identifies suggested NIST Framework priorities for each type.
- Provides a set of questions and use cases for broadcast companies to use in applying the framework to their business.









NIST Sub-Category	Small Radio Station	TV Broadcast Station	Station Hub	Network Facility
ID.AM-1: Physical devices and systems within the organization are inventoried	Critical	Critical	Critical	Critical
ID.AM-2: Software platforms and applications within the organization are inventoried	Critical	Critical	Critical	Critical
ID.AM-3: Organizational communication and data flows are mapped		May Not be Critical	Critical	Critical
ID.AM-4: External information systems are catalogued			Critical	Critical
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	Critical	Critical	Critical	Critical
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Critical	Critical	Critical	Critical
ID.BE-1: Organization's role in the supply chain is identified and communicated			May be Critical	May be Critical
ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated			May be Critical	May be Critical
ID.BE-3: Priorities for organizational mission, objectives and actives are established and communicated		May be Critical	Critical	Critical

1.What are you trying to protect?

2.Who is responsible/involved in the process?

3. How do you tackle the Framework/ What do you do first?

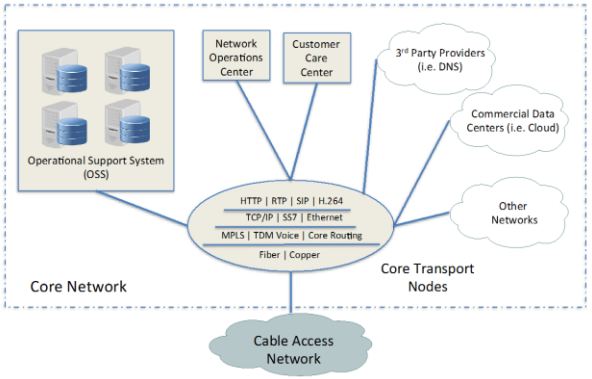
4.How did you determine what categories and subcategories are the most important /How did you implement the Framework guidance?

5. What are your plans for the future in regard to progressing in maturity?

Implementation Guidance and Resources

9.2 Cable Segment report:

- Focuses its scope on Cable Core Network as that which would have the greatest national or regional impact on service availability.
- Identifies all the NIST subcategories as in-scope and also identifies the 24 suggested highest priority practices for the Cable Segment.
- Includes a generic profile of the 24 priority practices with their anticipated outcomes.



High Priority Practices

Level 1	Level 2	Level 3
ID.AM-1: Physical devices and systems within the organization are inventoried	ID.AM-4: External information systems are catalogued	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
ID.AM-2: Software platforms and applications within the organization are inventoried	ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated	ID.RA-3: Threats, both internal and external, are identified and documented
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	ID.BE-5: Resilience requirements to support delivery of critical services are established	ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
ID.GV-1: Organizational information security policy is established	ID.GV-4: Governance and risk management processes address cybersecurity risks	PR.AT-1: All users are informed and trained
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties
PR.AC-1: Identities and credentials are managed for authorized devices and users	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	DE.CM-5: Unauthorized mobile code is detected
PR.AC-2: Physical access to assets is managed and protected	ID.RA-1: Asset vulnerabilities are identified and documented	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

For the use case below the assumption is for a large sized cable network operator.

A. Generic Profile Example

The table below illustrates a hypothetical profile as the result of an enterprise employing the methodology described in this report. The profile uses the 24 priority practices and augments them with anticipated outcomes. The anticipated outcomes provide a means for tracking the overall implementation of the profile.

Prioritized Practice	Anticipated Outcomes
ID.AM-1: Physical devices and systems within the organization are inventoried	Inventory of physical devices and systems in direct support of critical (core) infrastructure is completed.
ID.AM-2: Software platforms and applications within the organization are inventoried	Software platforms and applications in direct of support of critical (core) infrastructure are completed.
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	Prioritization of resources in direct support critical (core) systems is accomplished and in effect.
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Dependencies and critical functions are identified and supported to ensure dependencies are met.
ID.GV-1: Organizational information security policy is established	Security policy in place.

Implementation Guidance and Resources

9.3 Satellite Segment report:

- Provides a suggested list of NIST subcategories that apply to the segment along with their application, difficulty to apply and effectiveness.
- Includes an illustrative use case on how the NIST Identify, Protect, Detect, Respond, and Recover Framework can be used.
- Links to references of interest to the Satellite Segment.

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
		ID.RA-3: Threats, both internal and external, are identified and documented		2	3
		ID.RA-4: Potential business impacts and likelihoods are identified	Business can be read to include both operations and business development, or can be limited just to business impacts. Focus here is on impact to mission critical operations, not overall business.	2	3
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk		2	4
		ID.RA-6: Risk responses are identified and prioritized		2	4
Protect (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are managed for authorized devices and users		3	4
		PR.AC-2:Physical access to assets is managed		5	4

8. Appendix: Informative References

DoD 8581.01 — Information Assurance Policy for Space Systems Used by the Department of Defense; http://www.dtic.mil/whs/directives/corres/pdf/858101p.pdf
NIST SP 800-53 — Recommended Security Controls for Federal Information Systems; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
FIPS Publication 200 — Minimum Security Requirements for Federal Information and Information Systems; http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
NIST SP 800-30 — Guide for Conducting Risk Assessments; http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
ISO/IEC 27001 — Information security management systems — Requirements; http://www.iso.org/iso/catalogue_detail?csnumber=54534
ISO/IEC 27002 — Code of practice for information security management; http://www.iso.org/iso/catalogue_detail?csnumber=54533
NIST SP 800-37 — Guide for Applying the Risk Management Framework to Federal Information Systems; http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
Department of the Navy Chief Information Office (DON CIO) Acquisition Information Assurance Strategy; http://www.doncio.navy.mil/ContentView.aspx?id=4180

Implementation Guidance and Resources

9.4 Wireless Segment report:

- Provides a suggested list of NIST subcategories in scope for large organizations in the segment, and lists the top, mid and tertiary priorities.
- Lays out an illustrative use case and a generic profile with top priority subcategories and their corresponding outcomes applied to the segment.
- Includes challenges and links to references of interest specific to the Wireless Segment.

Subcategory Priority Analysis

Top Priority Subcategories	Mid-Tier Priority Subcategories	Tertiary Priority Subcategories
ID.AM-1: Physical devices and systems within the organization are inventoried	ID.AM-4: External information systems are catalogued	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
ID.AM-2: Software platforms and applications within the organization are inventoried	ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated	ID.RA-3: Threats, both internal and external, are identified and documented
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.GV-1: Organizational information security policy is established	ID.BE-5: Resilience requirements to support delivery of critical services are established	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	ID.GV-4: Governance and risk management processes address cybersecurity risks	PR.AT-1: All users are informed and trained
ID.GV-3: Legal and regulatory	ID.RA-5: Threats, vulnerabilities,	PR.IP-1: A baseline configuration of

7.7 Challenges to Overcome

7.7.1. As it relates to challenges to be overcome, the Wireless Segment defers to the conclusions defined in this report by the Barriers Feeder Sub-group, and adds the following wireless specific items:

7.7.1.1. The threat landscape in wireless varies and is different from traditional wireline or other segment environments and therefore use and conformity to the NIST Framework will vary and must be adapted for wireless entities.

7.7.1.2. The diversity of technology (i.e. 2G, 3G, 4G and WiFi) serves to create a complex environment that is global in scope where mobile devices can roam anywhere in the United States, and from the United States to other countries around the globe, and

7.7.1.3. The wireless ecosystem is highly diversified across OEMs, platform providers, Operating System providers, service providers and Over-the-top providers

Implementation Guidance and Resources

9.5 Wireline Segment report:

- Identifies suggested priority subcategories, and lays out a generic profile along with their anticipated outcomes.
- Analyzes the NIST subcategories for applicability to the segment, its application, criticality and difficulty to implement.
- Provides a crosswalk of NIST framework to CSRIC best practices.

Prioritized Practice	Anticipated Outcome
ID.AM-1: Physical devices and systems within the organization are inventoried	Inventory of physical devices (Critical Assets)
ID.AM-2: Software platforms and applications within the organization are inventoried	Inventory of software platforms and applications
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	Assets in Section 3 are classified according to criticality and business mission
ID.GV-1: Organizational information security policy is established	Security Policy is defined
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Documented security roles and regular coordination between internal and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Legal and regulatory requirements are established, organizational resources identified to manage and update as needed

Sub Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
	Is the function, category, sub-category in scope as a best practice for the critical infrastructure "systems and assets" determined by the sub-group (wireline, wireless, satellite, broadcast or cable)? (In-scope or Out-of-Scope).	Explanation of how the function, category, subcategory applies to the critical infrastructure as defined by the sub-group (wireline, wireless, satellite, broadcast or cable).	Criticality of the given function, category and subcategory on scale of 1 to 5 by segment. (Scale: 5= Extremely Critical, 4 = Very Critical, 3= Somewhat Critical, 2 = Slightly Critical, 1 = Not at all Critical).	Difficulty for the implementation of the function, (Includes factors such as costs and barriers to implementation). (Scale: 5= Not at all Difficult, 4 = Slightly Difficult, 3= Somewhat Difficult, 2 – Very Difficult, 1 – Extremely Difficult).
ID.AM-1: Physical devices and systems within the organization are inventoried	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
ID.AM-2: Software platforms and applications within the organization are inventoried	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
ID.AM-3: Organizational communication and data flows are mapped	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
ID.AM-4: External information systems are catalogued	In Scope	Critical infrastructure or as part of cyber risk management program.	4	2
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3


Q&A