CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4: Final Report
March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY

CSRIC IV Working Group 4 (WG4) was given the task of developing *voluntary mechanisms* that give the Federal Communications Commission (FCC) and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks across the enterprise.[1] WG4 also was charged with providing implementation guidance to help communication providers use and adapt the voluntary NIST Cybersecurity Framework[2] (hereinafter "NIST CSF").

Working Group 4 began its work shortly after the Communications Sector[3] completed a highly collaborative, multi-stakeholder process that resulted in the NIST CSF Version 1.0[4] that was called for in the President's Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.[5] The sector's participation in CSRIC WG4 was seen as an opportunity to assume the leadership urged by FCC Chairman Tom Wheeler in a speech delivered to the American Enterprise Institute in June 2014.[6] By building on the cross-sector NIST CSF and by framing its applicability to five major communications industry segments, the Working Group was able to formulate and commit to several voluntary mechanisms that provide the macro-level assurances sought by the FCC. Moreover, these mechanisms, combined with the insights, tools, guidance, and fact-based analyses developed by over 100 cybersecurity professionals who participated in a year-long effort to produce this report, validate the advantages of a non-regulatory approach over a prescriptive and static compliance regime.[7]

WG4 organized itself into five segment subgroups representing the five key parts of the communication industry. Their representatives were encouraged to pursue independent evaluations of the CSRIC WG4 charge based on their own operating environments. The five segments included:

---

[1] *See* Federal Communications Commission, *CSRIC IV Working Group Descriptions and Leadership* (2013), *available at* http://transition.fcc.gov/pshs/advisory/csric4/wg_descriptions.pdf.

[2] *See* National Institute for Standards and Technology, *Framework for Improving Cybersecurity*, 79 FR 9167 (Feb. 18, 2014) [hereinafter *NIST CSF*], *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[3] For purposes of this report, the "Communications Sector" is comprised of five industry segments including broadcast, cable, satellite, wireless, and wireline network service providers.

[4] *See NIST CSF*.

[5] *See* Exec. Order No. 13,691, *Promoting Private Sector Cybersecurity Information Sharing*, 80 FR 9347 (Feb. 13, 2015) [hereinafter *EO 13691*].

[6] *See* Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute, June 12, 2014, *available at* http://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc [hereinafter *Chairman Wheeler's Remarks*] ("[T]he network ecosystem must step up to assume new responsibility and market accountability for managing cyber risks.").

[7] *Id*. (statement of Chairman Tom Wheeler) ("[W]e 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.").

- Broadcast: There are more than 15,000 radios and 1,700 televisions broadcasting facilities in the United States, providing news, emergency information and other programming services over the air to consumers.[8]

- Cable: The cable industry is composed of approximately 7,791 cable systems[9] that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service.

- Satellite: Satellite communications systems use a combination of space-based infrastructure and ground equipment capable of delivering data, voice, video, and broadcast communications to any person in the U.S., its territories, and anywhere on the globe.

- Wireless: The Wireless industry delivers advanced wireless broadband services that include data, voice and video to more than 335 million active wireless-devices nationwide, including more than 175 million smartphones, 25 million tablets, and 51 million data-only devices.[10] There are approximately 160 facilities-based wireless carriers[11] in United States that operate and maintain more than 304,360 cell sites[12] that collectively provide the most advanced 4G technology deployment in the world.

- Wireline: Over 1,000 companies offer wireline, facilities-based communications services in the United States.[13] Wireline companies serve as the backbone of the Internet.

WG4 also established five "feeder" subgroups to engage in a deeper, more focused analysis of subject matter areas that would help the communications sector segments evaluate their cybersecurity risk environment, posture, and tolerance. To ensure that the voluntary mechanisms and sector guidance were grounded in facts, thoughtful judgments, and practical in their design, the following "feeder" topics were examined:

- Cyber Ecosystem and Dependencies
- Top Threats and Vectors
- Framework Requirements and Barriers

---

[8] National Association of Broadcasters, *Legislative Priorities 111th Congress*, 4, *available at* http://nab.org/documents/advocacy/NAB_111th_Legislative_Priorities.pdf.
[9] *See* U.S. Communications Sector Coordinating Council, *The Communications Sector*, http://www.commscc.org/ (last visited March 13, 2015).
[10] Cellular Telephone Industries Association (CTIA), *Wireless Industry Indices Report - Year-End 2013* 133 (June 2014).
[11] Federal Communications Commission, *Local Telephone Competition: Status as of December 31, 2013*, 29 (Oct. 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0219/DOC-329975A1.pdf.
[12] Cellular Telephone Industries Association ('CTIA'), *Wireless Annual Wireless Industry Survey*, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited Mar. 13 2015).
[13] *See id*.

- Small and Medium Businesses
- Measurements

Each of the segment subgroups, informed by the findings of the topical feeder subgroups, evaluated the applicability of the NIST Cybersecurity Framework's 98 subcategories to their segment, prioritized the applicable subcategories on an illustrative basis, and assessed the challenges of implementation and effectiveness for each applicable subcategory. The segment and feeder subgroup findings and resulting NIST Cybersecurity Framework implementation guidance are contained in the appendices to this report.

The key macro-level assurances developed by WG4 were designed to demonstrate how communications providers are appropriately managing cybersecurity risks through the *application of the NIST Cybersecurity Framework*, or an equivalent construct. The FCC described the desired characteristics of the assurances as:[14]

- Tailored by individual companies to suit their unique needs, characteristics, and risks;
- Based on *meaningful indicators* of successful cyber risk management; and
- Allowing for meaningful assessments both internally and externally.

A. Voluntary Mechanisms

As evidence of the Communications Sector's commitment to enhance cybersecurity risk management capabilities across the sector and the broader ecosystem, and to promote use of the NIST CSF, CSRIC recommends **three new voluntary mechanisms** to provide the appropriate macro-level assurances:

- **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)[15] administered by the Department of Homeland Security (DHS);
- **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
- Active and dedicated **participation in DHS' Critical Infrastructure Cyber Community C³ Voluntary Program,**[16] to help industry increase cybersecurity risk management awareness and use of the Framework.

[14] *See supra* note 1, at 4.
[15] *See* Department of Homeland Security, *Protected Critical Information Program*, http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program (last visited Mar. 13, 2015) [hereinafter *PCII Program*].
[16] *See* Department of Homeland Security, *About the Critical Infrastructure Cyber Community C³ Voluntary Program*, http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program (last visited Mar. 13, 2015) [hereinafter *DHS C³ Voluntary Program*].

1) ***Confidential Company-Specific Meetings:*** The sector supports the development of a voluntary program for periodic meetings, or an alternative means of communications among the FCC, DHS, and individual companies that agree to participate. The purpose of these meetings would be to discuss efforts by the organizations to develop risk management practices consistent with the NIST Cybersecurity Framework or equivalent constructs. During the meetings, the participating 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.

2) ***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. WG4 initiated the "Measurement" subgroup to analyze how to best demonstrate the overall state of cybersecurity within the communications sector. The Measurement subgroup recommends that the Communications Sector Coordinating Council (CSCC), as the official interface for the sector can include information on the cybersecurity of critical communications network infrastructure in future drafts of the Sector Annual Report (SAR) 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.

3) ***Active Participation in DHS C³ Outreach and Education:*** The Department of Homeland Security oversees a program that it created in response to a directive contained in Executive Order 13636. DHS created the Critical Infrastructure Cyber Community C³ Voluntary Program as part of what it describes as an "innovative public-private partnership designed to help align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks."[17] The Program emphasizes three C's:

[17] *See DHS C³ Voluntary Program*.

- *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 has already participated in development activities and was recently featured in the first of a series of C³ webinars where CSRIC Working Group 4 activities were described.[18] To advance the use of the Framework through the implementation guidance contained in this report and from other sources, the communications sector will develop a series of webinars and other reference materials. 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.

B. Guidance to Individual Companies on the Use of the NIST Framework

Charged with providing implementation guidance to facilitate the use and adaptation of the voluntary NIST Cybersecurity Framework by communications providers, the WG4 members developed and applied a variety of analytical tools and methods that could serve as a primer for companies when reviewing their own risk management processes. The NIST CSF Version 1.0 offers organizations direction when they are implementing or enhancing their cybersecurity risk management program. In addition, the report provides informative references that include leading cybersecurity protocols, resources, and tools. NIST emphasized the "voluntary" nature of the Framework, noting that it is designed to use "business drivers to guide cybersecurity activities" and to "manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[19]

While this report incorporates findings, conclusions, and recommendations related to guiding individual companies on the use of the Framework, many communications companies have long-standing and mature cybersecurity risk management capabilities and others within the communications sector did not wait for this report to be finalized before beginning their evaluation of the applicability of the Framework components to their enterprise. Reducing cybersecurity risk by implementing widely recognized standards and guidelines[20] has been a hallmark of communications industry practice, and is supported by

[18] *See* Department of Homeland Security, *C Cubed Voluntary Program*, https://share.dhs.gov/p1qqp8dvu34/ (last visited Mar. 13, 2015).
[19] *See NIST CSF*.
[20] *See* Government Accountability Office, *Critical Infrastructure Protection – Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use* (Dec. 2011), *available at* http://www.gao.gov/assets/590/587529.pdf.

exceptionally high levels of service availability.[21] Notwithstanding this fact, the NIST Framework is a seminal document in organizing risk management activities across a broad global landscape. Over 100 professionals from across the communications sector and the broader stakeholder community have worked tirelessly over the past 12 months to produce a report with recommendations on Framework use which should have immediate and practical value for individual sector companies and other key stakeholders.

1) ***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.

   When managing cybersecurity risks, it is essential to incorporate a risk governance process into the program. The key objective is to ensure that an inclusive, independent, and holistic assessment of the current and future enterprise risk posture is routinely undertaken, and to align the enterprise's business mission with sound and effective cybersecurity practices, protocols, and tools. 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.

2) ***NIST CSF Implementation Recommendations*:** The WG4 industry segment subgroup reports in the appendices to this report provide concrete guidance on how to use the Framework can bolster cyber readiness. Each WG4 segment subgroup report surveys infrastructure core assets and critical services, and also employs use cases, all with the aim of offering guidance in how to incorporate the risk management

[21] *See* Federal Communications Commission, *Network Outage Reporting System (NORS)*, http://transition.fcc.gov/pshs/services/cip/nors/nors.html (last visited Mar. 13, 2015) (a web-based filing system through which communications providers covered by C.F.R. Part 4 reporting rules submit outage reports to the FCC, and allows the FCC to perform analyses and studies of the communications disruptions reported).

protocols and practices referenced in the Framework with the operating environment of the respective industry segment.

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[22] 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.

C. Communication Sector Commitment to Advancing Cybersecurity Risk Management

While this WG4 CSRIC report represents a major milestone, the WG4 members acknowledge that we are not at the finish line. Efforts to help enterprises manage cybersecurity risk must be continuous and ongoing to adapt to a continually changing ecosystem and threat landscape. While the sector will actively promote use of the Framework through ongoing and anticipated work in multiple venues, the Working Group members are also cognizant that each enterprise must decide how to utilize and implement the Framework or an equivalent risk management construct. The mechanisms and assurances highlighted below are intended to demonstrate the sector's commitment to industry-led solutions based on close collaboration with our government partners and regulators.

[22] *See Infra* §9.10 Threat Intelligence Handling Model.

II. INTRODUCTION

Working Group 4 marked a fundamental CSRIC shift to a risk management construct that aligns with the five functions identified in the NIST Framework (i.e., Identify, Protect, Detect, Respond and Recover). Many in government and the private sector have come to understand that the traditional multi-year CSRIC review cycles can no longer keep pace with the accelerating deployment of new network and edge technologies across the ecosystem along with the rapid advancements in increasingly inexpensive, perishable, and more sophisticated cyber threats.

With the issuance of the 2013 Presidential Executive Order 13636, "Improving Cybersecurity Critical Infrastructure," and the subsequent 2014 release of the NIST Cybersecurity Framework Version 1.0, there is renewed emphasis on cybersecurity risk management as the foundation for protecting our nation's critical infrastructure. The U.S. government has clearly endorsed development of a voluntary, risk-based model that enables organizations to prioritize and implement solutions based on informed, enterprise-tailored, business-driven considerations. The government acknowledged that cost-effectiveness is an important consideration when evaluating new security measures and recognizes that incentives may be required in certain circumstances. It is also generally acknowledges that meaningful methods to assess the costs and benefits of cybersecurity investment are often elusive.

In a June 2014 speech to the American Enterprise Institute, FCC Chairman Tom Wheeler endorsed the risk management approach stating that "...companies must have the capacity to assure themselves, their shareholders and boards – and their nation – of the sufficiency of their own cyber risk management practices. These risk assessment approaches will undoubtedly differ company by company. But regardless of the specific approach a company might choose, it is crucial that companies develop methodologies that give them a meaningful understanding of their risk exposure and risk management posture that can be communicated internally and externally. That is what we are asking our stakeholders to do."[23]

To set a path for widespread use of risk management processes by sector enterprises, WG4 studied the Framework components and the factors that are most likely to impact enterprise-level risk management decisions. The project was structured around five independent industry segments based on their common operating environments and architectures. The segments included Broadcast, Cable, Satellite, Wireless, and Wireline. Each segment made its own determination as to what critical infrastructure should be categorized as "in-scope" or "out-of-scope" and which of the NIST categories and sub-categories were most critical to protecting that infrastructure. Each group chose criteria to prioritize the risk management processes. The analyses were intended to be illustrative examples of how individual companies in each segment could go about assessing and prioritizing the framework components.

The industry-based segments were supported by the five subject-matter oriented "feeder" groups. The "Requirements and Barriers" group evaluated the operations and technology

[23] *See Chairman Wheeler's Remarks* at 7.

requirements and the barriers associated with each of the 98 NIST sub-categories. The "Cyber Ecosystem" group examined the ecosystem dependent landscape for communications providers and the most prominent threats that are flowing across the Internet stack.[24] The "Top Cyber Threats" team evaluated the evolving threat environment and identified enterprise-level processes and a community threat model that could be used by the communications sector to share information and coordinate response and recovery activities. The "Measurement" group examined challenges associated with obtaining reliable indicators of causality (i.e., risk process/risk reduction) and effective mechanisms to address stakeholder interests in key indicators. And, since many providers classify as small and medium sized enterprises, the "Small and Medium Business" group looked at their unique challenges and provided guidance on Framework related approaches suitable for such organizations.

The Communications Sector continues to be a leader in cybersecurity because providers offer a broad array of communication services to some of the most demanding customers in the world. For all communication providers, ensuring the integrity and resilience of their networks and the availability of services is a mission critical responsibility. Meaningful indicators of critical service availability, reliability, resiliency, and integrity show their success in this arena.

However, across the broad spectrum of providers there is a range of risk management capabilities that may often be associated with providers' ability to recover the cost of cybersecurity investment in a highly competitive market. While enterprise size is often associated with risk management capabilities, it is not always the only factor. In fact, an organization's unique threat environment, its understanding of vulnerabilities, its business strategy, and its overall tolerance of risk can influence investment decisions.

This report provides a valuable roadmap for companies in our sector to validate their existing risk management processes and/or enhance their capabilities based on an ongoing evaluation of their threats, vulnerabilities, and risk tolerance. The feeder subgroup's contributions, including their analyses, findings, and implementation guidance, along with the segment subgroups' implementation guidance and assessment of the applicability of the NIST Cybersecurity Framework's 98 subcategories to each segment, are presented as appendices to this report and can be used by companies, large and small, to further guide their use of the NIST Cybersecurity Framework in managing their cybersecurity risks. Equally important, the WG4 members propose a set of "voluntary mechanisms" and FCC recommendations that leverage the communication sectors' existing organizational structure, experience, and cybersecurity risk management sector leadership to provide the requested macro-level assurances. The report concludes by suggesting the FCC coordinate with other departments and agencies to promote education and awareness of the cybersecurity risks inherent in critical communications infrastructures, and promote the voluntary steps the communication sector takes to manage their cybersecurity risks.

---

[24] *See* Wikipedia, *Structure of the Internet: TCP IP protocol stack*, http://en.wikibooks.org/wiki/A-level_Computing/AQA/Computer_Components,_The_Stored_Program_Concept_and_the_Internet/Structure_of_the_Internet/TCP_IP_protocol_stack (last visited Mar. 13, 2015).

III. BACKGROUND

On February 12, 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[25] which set in motion a wide range of government initiatives designed to advance the nation's cybersecurity resiliency. In its policy introduction, the Order articulated societal values to be promoted and reinforced the public-private partnership construct as the mechanism for making progress:

> "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."[26]

A key component of the President's Executive Order was the assignment given to the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, to lead the development of a "Cybersecurity Framework" to reduce cyber risks to critical infrastructure. Critical infrastructure is defined as, "…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[27]

NIST was given a list of what should be included in the final Framework and had one year to complete its work. The Order gave explicit instructions regarding the characteristics of the Framework and how it was to be used:

> "The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies,

[25] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013) [hereinafter *EO 13636*].
[26] *Id.* at §1: Policy.
[27] *Id.* at §2: Critical Infrastructure.

> procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework."[28]

To encourage use of the Cybersecurity Framework, the Department of Homeland Security (DHS) was ordered to establish a voluntary program to support owners and operators of critical infrastructure ("and any other interested entities") that wanted to use the Framework as part of an existing or new risk management program. Sector-Specific Agencies were instructed to coordinate with the Sector Coordinating Councils to "…review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."[29]

The Communications Sector organized its participation in the Framework development effort through the CSCC, and Council representatives participated in all six NIST workshops held at major research universities throughout the country.[30] Industry representatives participated on panels, submitted comments, and had extensive dialogue with the Framework development team.

On February 12, 2014, NIST released the Framework for Improving Critical Infrastructure Version 1.0[31] stating that it "…enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[32] The authors noted that the "Framework is not a one-size-fits all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, and different risk tolerances – and how they implement the practices in the Framework will vary."[33] The Cybersecurity Framework provides guidance on how it can be used by an organization to enhance an existing program or to create a new risk management program.

The Framework initiative was aligned with the efforts of the FCC's Communications Security Reliability and Interoperability Council (CSRIC) IV. The CSRIC IV charter called for an update of the cybersecurity best practices that had been developed as part of CSRIC II Working Group 2A: Cyber Security Best Practices. That effort ended in March 2011 and produced 397 best practices covering a wide range of technology platforms and services.[34] At the urging of

---

[28] *Id.* at §7: Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.
[29] *Id.* §8: Voluntary Critical Infrastructure Cybersecurity Program.
[30] *See* National Institute of Standards and Technology, *Cybersecurity Framework - Workshops and Events*, http://www.nist.gov/cyberframework/cybersecurity-framework-events.cfm (last visited Mar. 13, 2015).
[31] See *NIST CSF*.
[32] *Id.* at 1.
[33] *Id.* at 2.
[34] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council II, *Working Group 2A Cybersecurity Best Practices – Final Report* (2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

industry representatives, the FCC agreed that CSRIC IV Working Group 4 should begin work immediately following the February 2014 release of the Framework because industry was a significant contributor of resources to the multi-stakeholder collaborative process that was being coordinated by NIST. It was also understood that the subsequent CSRIC IV Working Group 4 effort would benefit from being informed by the NIST process and final product.

To effectively execute a project of this scope, the Working Group Co-Chairs established a Leadership Team to ensure that qualified resources were appropriately applied to work efforts and that the work products aligned with the overall objectives of the effort. This Leadership Team evolved to include 20 individuals that served as segment and feeder group leaders and a Technical and Policy Advisory Board that included senior representatives from NIST, the White House National Security Office, and the FCC. With over 100 volunteers representing the five major industry segments as well as stakeholders from other sectors, academia, and state and federal government, this was the largest Working Group effort undertaken in the history of the CSRIC and the Network Reliability and Interoperability Council (NRIC) (i.e., CSRIC's predecessor).

A. CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	**Chair or Co-Chairs: Working Group 4**	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Next Generation 911	Working Group 2: Wireless Emergency Alerts	Working Group 3: EAS	**Working Group 4: Cybersecurity Risk Management and Best Practices**	Working Group 5: Server-Based DDoS Attacks	Working Group 6: Long-Term Core Internet Protocol Improvements	Working Group 7: Legacy Best Practice Updates	Working Group 8: Submarine Cable Landing Sites	Working Group 9: Infrastructure Sharing During Emergencies	Working Group 10: CPE Powering

B. Leadership Team

C. Working Group 4 Team Members

Working Group 4 consists of the members listed below.

Name	Company
Robert Mayer (Co-Chair)	**USTelecom Association**
Brian Allen (Co-Chair)	**TWCable**
Donna Dodson (Senior Tech Advisor)	**National Institute of Standards and Technology**
Emily Talaga (Senior Economic Advisor)	**Federal Communication Commission**
Vern Mosley (FCC Liaison)	**Federal Communication Commission**
Adrienne Abbott	**Nevada EAS Chair**
Anthony Acosta	**Northrop Grumman**
Michael Alagna	**Motorola Solutions**
Carl Anderson	**Van Sco Yoc Associates**

Nadya Bartol	Utilities Telecom Council
James Bean	Juniper Networks
Chris Boyer	AT&T
Chuck Brownawell	Sprint Corporation
Lois Burns	PA Public Utility Commission
Ingrid Caples	Department of Health and Human Services
Joel Capps	Ericsson
Lisa Carnahan	NIST
Dan Cashman	FairPoint
Nneka Chiazor	Verizon
Larry Clinton	Internet Security Alliance
Edward Czarnecki	Monroe-Electronics
Kate Dean	USISPA
Paul Diamond	CenturyLink
Martin Dolly	AT&T (representing ATIS)
Tanner Doucet	Internet Security Alliance
Seton Droppers	PBS Technology & Operations
Victor Einfeldt	Iridium
Russell Eubanks	Cox Communications, Inc
Paul Ferguson	Internet Identity
Inette Furey	Department of Homeland Security
Andrew Gallo	George Washington University
Chris Garner	CenturyLink
Michael Geller	Cisco (representing ATIS)
My K. Gomi	NTT America
Jessica Gulick	CSG International
Stacy Hartman	CenturyLink
Mary Haynes	Charter
Chris Homer	PBS
Charles Hudson, Jr	Comcast
Wink Infinger	Florida Department of Management Services
Chris Jeppson	Consolidated

Susan Joseph	CableLabs
Franck Journoud	Oracle
Merike Kaeo	Internet Identity
Kevin Kastor	Consolidated
John Kelly	Comcast
Danielle Kriz	Information Technology Industry Council
Rick Krock	Alcatel-Lucent
Jeremy Larson	SilverStar
Greg Lucak	Windstream
Ethan Lucarelli	Wiley Rein LLP
Daniel Madsen	US Bank
John Marinho	CTIA
Heath E. McGinnis	Verizon
Donna Bethea Murphy	Iridium
Paul Nguyen	CSG International
Jorge Nieves	Comcast
Michael O'Reirdan	Comcast (representing MAAWG)
Martin Pitson	Telesat
Joel Rademacher	Iridium
J. Bradford Ramsay	NARUC
Alan Rinker	Boeing
Chris Roosenraad	TWCable
Tony Sager	Council on Cybersecurity
Harold Salters	T-Mobile
Brian Scarpelli	TIA Online
Karl Schimmeck	SIFMA
J. J. Shaw	O3b Government
Ray Singh	ACS
Tom Soroka	USTelecom Association
Craig Spiezle	Online Trust Alliance (OTA)
Matt Starr	CompTIA
Bill Taub	Cablevision Systems Corporation

Robert Thornberry	**Bell Labs/Alcatel-Lucent**
Sheila Tipton	**Iowa Utilities Board**
Matt Tooley	**NCTA**
Bill Trelease	**CTO Delhi Telephone Company**
Colin Troha	**CSG Invotas**
S. Rao Vasireddy	**Alcatel-Lucent (TIA representative)**
Joe Viens	**TWCable**
Christian Vogler	**Gallaudet University**
Jesse Ward	**NTCA**
Errol Weiss	**Citi**
Kathy Whitbeck	**Nsight/Cellcom**
Jack Whitsitt	**National Electric Sector Cybersecurity Organization**
Kelly Williams	**National Association of Broadcasters (NAB)**
Shawn Wilson	**VeriSign**
Pamela A. Witmer	**PA Public Utility Commission**
Shinichi Yokohama	**NTT**

Table 1 - List of Working Group Members

IV. OBJECTIVE, SCOPE, AND METHODOLOGY

A. Objective

The NIST Framework was designed as a multi-sector baseline document that individual sectors could tailor in ways that might make it more relevant and useful to organizations operating within their sector. In the case of the expansive communications sector, a segment-specific analysis was deemed to be more productive (i.e., broadcast, cable, satellite, wireless, and wireline segments). Consequently WG4 participants focused on developing segment-specific cyber risk management approaches and guidance that would serve as a foundation for producing the assurances called for in the CSRIC IV Working Group 4 description. As outlined below, the Working Group's assurances and recommendations build upon the foundational work in the Framework Version 1.0 and are supported by fact-based analyses and informed judgments in areas that are critical to the ability of the communications sector and enterprises to evolve their cybersecurity risk management profiles.

Working Group 4's efforts were designed to provide individual service providers an ability to assure themselves, their shareholders or owners, their boards, and external stakeholders that they are taking appropriate steps to manage cybersecurity risk. While individual

enterprises are given flexibility on how they use the Framework, Working Group 4 focused on tailoring the Framework to the unique considerations of the segments and providing macro-level analyses and mechanisms to sustain risk-management capabilities.

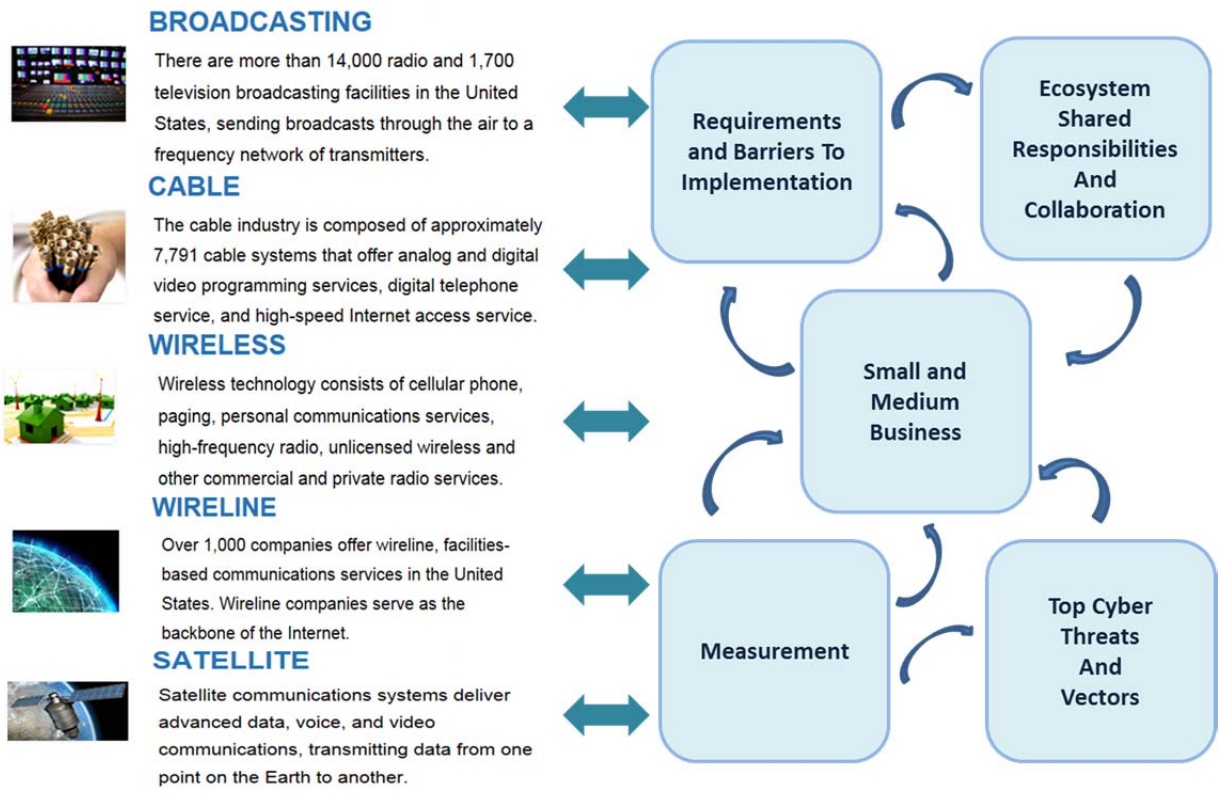
B. Scope

Working Group 4 was tasked with producing a practical, cost-effective, and segment-tailored model of risk management with meaningful indicators to communicate assurances to internal and external stakeholders. To facilitate sector-wide use of the framework or an alternative risk management construct, it was necessary to evaluate the five Framework functions, 22 categories, 98 sub-categories, and the factors that would impact an enterprises' decision to adopt or enhance a particular risk management process. Additionally, the Working Group developed, tested, and utilized an analytical template that an enterprise could adopt to prioritize its risk management activities based on a critical examination of considerations that would be relevant to its unique circumstances.

C. Methodology

The project methodology was designed to provide strong factual and analytical underpinnings to support service provider's cybersecurity risk management activities. The project was structured as an iterative process to ensure that segment analyses were constantly evaluated as new feeder group input was received. That process is illustrated below.

Figure 1 - Segment Analysis Process



The effort began with the development of an analytical template that each of the segments used to evaluate how the Framework's structure might be applied to an enterprise operating in its segment.

The segment teams were first asked to determine whether a particular Framework Function, Category or Sub-Category was deemed to be "in-scope or out-of-scope" for purposes of prioritizing risk management processes. The five segments relied on work completed as part of the 2012 National Sector Risk Assessment for Communications, which examined the common operating environments of the five segments and identified core infrastructure and associated critical services. Each segment made an independent determination as to which Framework Categories and sub-categories met the criteria for being identified as in or out-of-scope. The flexibility afforded to the segment teams was

consistent with the Framework's emphasis on flexibility and was designed to be illustrative for individual companies that might make similar scoping determinations.

Figure 2 – Segment Scoping Analysis

			Scoping Analysis	
			In Scope/Out of Scope	Application
		Response Level:	By Segments and Sub-Groups	By Segments and Sub-Groups
Function	Category	Sub-Category (only as needed)	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).
	Asset management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried		
		ID.AM-2: Software platforms and applications within the organization are inventoried		
		ID.AM-3: Organizational communication and data flows are mapped		
		ID.AM-4: External information systems are catalogued		
		ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value		
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers,		

Once a process was determined to be in-scope, the next analytical component was identification and ranking of criteria. Segments were free to select relevant criteria among a set that included the criticality of a particular process, the difficulty associated with implementing a particular process, and how effective it could be in mitigating cybersecurity risk.

Figure 3 – Segment Identification and Ranking of Criteria

Prioritization/Sorting		
Criticality	Difficulty	Effectiveness
Segments/Feeder Sub-Groups	Segments/Feeder Sub-Groups	Segments/Feeder Sub-Groups
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, category and sub-category on scale of 1 to 5 by segment (Includes factors such as costs and barreirs analysis to the right). (Scale: 5= Not at all Difficult, 4 = Slightly Difficult, 3= Somewhat Difficult, 2 = Very Difficult, 1 = Extremely Difficult).	Degree of effectivenss for the implementation of the function, category and sub-category on scale of 1 to 5 by segment. (Scale: 5= Extremely Effective, 4 = Very Effective, 3= Somewhat Effective, 2 = Slightly Effective, 1 = Not at all Effective).

How to prioritize Framework processes rested on work that was developed by the feeder groups. Once a determination was made regarding the "criticality" of a particular process, a structured basis for determining difficulty was developed by the "Requirements and Barriers" Feeder Group. For each of the 98 sub-categories included in the Framework, a team reviewed the operational and technological requirements associated with

implementing that specific risk management process. Understanding these requirements and the potential barriers or challenges for organizations of varying size and scope was critical to making supportable arguments around difficulty.

Figure 4 – Requirements and Barriers

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**Operational Requirement(s):**
	Organizations should monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and departments must be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations should classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations should only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations should collect data and track all activities with critical assets. This should include, but not limited to looging of all logins, applications used, files accessed/copied/downloaded, all doors opened, Internet connections/URLs / times these events occured and who conducted
	Technology Requirement(s):
	Access control / logging / disabling technologies and systems may have to be deployed to protect critical assets.
	Barriers:
	There will be an additional CAPEX cost to procuring Access control / logging / disabling technologies and systems.
	There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Access control / logging / disabling technologies and systems.

V. FINDINGS

Working Group 4 strived to do more than just develop a tool that communication providers can use to adapt the Framework in a voluntary, prioritized, and cost-effective fashion. The Working Group endeavored to break new ground in understanding cybersecurity risk management. As such, teams were established to address the unique considerations of small and medium enterprises in the sector, the ecosystem and dependencies that impacted risk, the threats and ways in which organizations can evolve capabilities as new threats arise, the barriers to implementing successful risk management regimes, and the appropriate mechanisms and measures to address a dynamic set of cyber conditions. This report demonstrates the communication sector's capability to address the evolving cyber threat through voluntary collaboration. This position is supported by the ongoing level of critical service availability, reliability, and resiliency across the communications industry.

The findings, as are the conclusions and recommendations, are organized around the five key areas of the Working Group 4 charge:[35] (1) macro-level assurances, (2) voluntary mechanisms, (3) use of the NIST Cybersecurity Framework or an equivalent construct, (4) meaningful indicators of successful cyber risk management, and (5) communications sector implementation guidance for using the NIST Cybersecurity Framework.

A. Macro-Level Assurance Findings

The following summary findings address the Working Group 4 charge to provide macro-level assurance that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks.

- CSRIC found that adapting the voluntary Framework is an effective way to manage cybersecurity risk.
- Communications sector members share detailed threat intelligence information with appropriate stakeholders, within the confines of existing law.
- Work is underway on the incentives category that is recognized in EO 13636 as an essential factor in improving critical infrastructure cybersecurity.
- Communications sector members are taking steps to advance their cybersecurity risk management practices, although variations exist with respect to levels of program development and implementation.
- The communications sector organizes its strategic, planning and operational cybersecurity activities through three respective entities: the National Security Telecommunications Advisory Council (NSTAC), the Communications Sector Coordinating Council (CSCC)/Government Coordinating Council (GCC), and the Communications Information Sharing and Analysis Center (Comm-ISAC).

[35] *See supra* note 1, at 4.

- Small and Medium Businesses (SMBs) have unique circumstances and challenges that may influence their approach to implementing the Framework and providing macro-level assurances.

B. Voluntary Mechanisms Findings

The following summary findings address the Working Group 4 charge to identify voluntary mechanisms to provide macro-level assurances.

- A static checklist methodology is not an effective defense, as it is limits the methods and tactics by which an organization can prepare for or respond to imminent and evolving threats.
- CSCC/GCC is an effective organizational structure for integrating a new initiative to evaluate how cybersecurity threats are measured at the sector level.
- Key government stakeholders have a legitimate interest in gaining information about cybersecurity threats to critical infrastructure and the effectiveness of cybersecurity risk management practices.

C. Use of the NIST Cybersecurity Framework or an Equivalent Construct Findings

The following summary findings address the Working Group 4 charge to provide macro-level assurances that demonstrate how communications providers are reducing cybersecurity risks through the use of the NIST Cybersecurity Framework or an equivalent construct.

- Use of a community model for threat intelligence or information sharing and analysis can help organizations in their quest to protect their critical infrastructure and critical data from future cyber threats.
- Use of the voluntary NIST CSF provides a consistent cybersecurity risk management approach and a common taxonomy to improve internal and external communications regarding cybersecurity risk management.
- Prior to the NIST CSF, many communications sector members already were actively engaged in equivalent processes to successfully manage cybersecurity risks.

D. Meaningful Indicators Findings

The following summary findings address the Working Group 4 charge to provide macro-level assurances that are based on meaningful indicators of successful cyber risk management.

- Meaningful indicators of successful (or unsuccessful) cyber risk management focus on measureable outcomes.
- It is difficult to measure the effectiveness of the communications sector's cybersecurity risk management processes in isolation, given its interdependencies on other critical infrastructure sectors.

E. Communications Sector Implementation Guidance Findings

The following summary findings address the Working Group 4 charge to give the communications sector guidance on how to implement using the NIST Cybersecurity Framework.

- The NIST Cybersecurity Framework is an effective mechanism to create a new risk management process or to enhance existing cybersecurity risk management processes.
- Cyber-attacks have been observed and mapped to every layer of the TCP/IP communication model, and subsequently against every identified category of the ecosystem. Cyber-attacks will continue to occur at every level of the TCP/IP communications model. It is important that all operators and vendors in every layer of the TCP/IP model conduct their operations with the appropriate level of cybersecurity diligence.
- The communications sector is part of a vast interdependent ecosystem that requires sharing cybersecurity responsibilities among a variety of stakeholders and depends on multiple non-communications sector ecosystem entities to make the communications infrastructure more secure.
- Further outreach is needed to ensure that the SMB community is engaged in the network risk management discussion generally, and aware of the benefits of the NIST Framework specifically.
- It is not a matter of "IF" a communications sector member will be attacked, but a matter of "WHEN" they will be attacked, and that threat knowledge is essential to protect against attacks.

VI. CONCLUSIONS

The conclusions drawn below align with the key task areas assigned to Working Group 4 and are supported by a yearlong effort involving substantial inquiries into cybersecurity activities at the enterprise, segment, and sector levels.

A. Macro-Level Assurance Conclusions

The following conclusions address the Working Group 4 charge to provide macro-level assurance that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks.

- No new regulations are needed or warranted to address conformity to the NIST Framework. Such a regulatory regime would spur a minimum standard, not maximum effort, and would undermine adaptability and innovation.
- Cyber threat information sharing results in efficient and scalable information that all parties can use to develop threat analyses and to make cyber risk management decisions.
- Progress on incentives is necessary to overcome many of the barriers identified in this report.
- The steps the communications sector members are taking to advance their cybersecurity risk management practices can be conveyed to relevant stakeholders with appropriate protections for security and market purposes. The NSTAC, CSCC/GCC, and Comm-ISAC are effective venues for information sharing and collaboration regarding reduction of cybersecurity risks, not only among its members but with other critical infrastructure sectors and government departments and agencies that are dependent upon the communications sectors' critical infrastructure and services.
- Special considerations and accommodations may be necessary for SMBs to implement the Framework and provide macro-level assurances to the FCC and the public.

B. Voluntary Mechanisms Conclusions

The following conclusions address the Working Group 4 charge to identify voluntary mechanisms that can be used to provide macro-level assurances.

- A checklist approach would prioritize compliance over an adaptable security risk-based management model that is required to address the evolving cyber threat landscape.
- Future requests for measurements by government agencies into the impact of cybersecurity threats to communications infrastructure would be most effectively managed by the CSCC/GCC.

- The communications sector can make external stakeholders more aware of its corporate and operational cybersecurity risk management measures through current communications sector venues that have the requisite protections.
- Voluntary mechanisms, including an industry SAR and periodic meetings with communications sector members, can provide macro-level assurance that communications providers are taking the appropriate measures to manage cybersecurity risks.

C. Use of NIST Cybersecurity Framework or Equivalent Construct Conclusions

The following conclusions address the Working Group 4 charge to provide macro-level assurances that demonstrate how communications providers are managing cybersecurity risks through the use of the NIST CSF or an equivalent construct.

- The introduction of the NIST CSF represents a major breakthrough in the ability to communicate cybersecurity risk management principles and processes and can be effectively employed by the communications sector and applied to other critical infrastructure sectors.
- The use of the NIST CSF will continue to evolve within the communications sector as more experience is gained and shared.
- Continued inter-agency and federal/state coordination and collaboration with industry in advancing the Framework is needed to avoid fragmentation of industry and government resources.

D. Meaningful Indicators Conclusions

The following conclusions address the Working Group 4 charge to provide macro-level assurances that are based on meaningful indicators of successful cyber risk management.

- Individual company malware infection rates, the number of hosted bots, and customer service complaints are not meaningful indicators of successful cyber risk management, as they are not outcome-based measures.
- The availability of the critical infrastructure to deliver critical services is an outcome-based measure and therefore a meaningful indicator of successful cyber risk management. If issues related to availability arise as a consequence of a cyber-incident, additional examination into reliability, resiliency, and integrity of core network critical infrastructure may need to be evaluated.
- Further analysis is required to determine whether a comprehensive and valid set of cybersecurity effectiveness metrics can be applied on a cross-sectorial basis.

E. Communications Sector Implementation Guidance Conclusions

The following conclusions address the Working Group 4 charge to give the communications sector guidance on implementing the NIST Cybersecurity Framework.

- Communications segment members will benefit from their review of this report and the analytical processes in the report that they can use to implement the NIST Framework or an equivalent construct.
- Use of the NIST CSF must remain flexible as "one size does not fit all," and companies should use the Framework in a way that is appropriate to their risk environment, posture, and tolerance.
- The communications sector is effectively advancing the use of the NIST CSF as evidenced by the industry's participation in development of this report.
- As evident in this report, small and medium communications sector members have unique challenges to overcome in the use of the NIST CSF.
- Communications sector members are one component of a vast landscape of interdependent critical infrastructure ecosystem stakeholders that requires a high degree of information sharing (consistent with applicable law) and collaboration to effectively manage cyber risk.
- Use of the voluntary NIST CSF or equivalent risk management construct across all ecosystem stakeholders will improve cybersecurity risk management.
- As it relates to the use of the NIST CSF, sharing information about experiences and lessons learned across the ecosystem will facilitate improvements in the further development of the Framework and cybersecurity risk management generally.
- Communications sector members, as well as other critical infrastructure sectors, can share detailed threat intelligence information with appropriate stakeholders, consistent with current law, and thus enable more efficient and scalable threat information gathering for cyber risk management decision-making.
- As NIST, DHS, the FCC, and industry continue their outreach, they should understand that a single method of outreach might not be sufficient for an SMB. A multi-faceted approach is necessary.

VII. RECOMMENDATIONS

The following recommendations are consistent with the Federal Advisory Committee Act (FACA)[36] 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.

A. Macro-Level Assurance Recommendations

The following recommendations address the Working Group 4 charge to provide macro-level assurance that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks.

- CSRIC recommends that the FCC 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.
- CSRIC recommends that the FCC 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.
- CSRIC recommends that the FCC further explore the considerations and accommodations that are required for SMB's to implement the NIST Cybersecurity Framework and provide macro-level assurances to the FCC and the public.

B. Voluntary Mechanisms Recommendations

The following recommendations address the Working Group 4 charge to identify voluntary mechanisms to provide macro-level assurances.

- CSRIC recommends that the FCC, in partnership with DHS, participate in periodic meetings with communications sector members, in accordance with PCII protections,[37] to discuss their cybersecurity risk management processes and their use of the NIST CSF or equivalent construct.
- CSRIC recommends that the FCC use the current communications sector organizational structure within the CSCC/GCC to deliver an industry Sector Annual Report (SAR) that addresses the effectiveness of communications sector cybersecurity risk management processes.

[36] *See* General Services Administration, *Federal Advisory Committee Act (FACA) Management Overview*, http://www.gsa.gov/portal/content/104514 (last visited Mar. 13, 2015).
[37] *See PCII Program* or another legally sustainable construct.

C. Use of NIST Cybersecurity Framework or Equivalent Construct Recommendation

This recommendation addresses the Working Group 4 charge to provide macro-level assurances that demonstrate how communications providers are managing cybersecurity risks through the NIST Cybersecurity Framework or an equivalent construct.

- CSRIC recommends that the FCC promote the voluntary use of the NIST CSF among all communications sector members, large and small, as well as across other critical infrastructure sectors that are interdependent with the communications sector.
- CSRIC recommends that the FCC work to coordinate and rationalize Framework related federal/state government initiatives to ensure efficient use of critical and scarce cybersecurity resources.
- CSRIC recommends that the FCC further incorporate an understanding of the changing threat landscape, sector ecosystem dependencies, and harmonization into previous CSRIC best practices and the NIST CSF.

D. Meaningful Indicators Recommendations

The following recommendations address the Working Group 4 charge to provide macro-level assurances that are based on meaningful indicators of successful cyber risk management.

- CSRIC recommends that the FCC adopt availability of the critical communications infrastructure as the meaningful indicator of cybersecurity risk management.
- CSRIC recommends that the FCC leverage the communications sectors' current organizational structure (i.e., CIPAC) to deliver an industry Sector Annual Report to address the proposed meaningful indicator and corporate and operational initiatives the communications sector is taking to manage cybersecurity risk.
- CSRIC recommends that the FCC, in partnership with DHS and NIST, promote continued industry participation in efforts to evaluate the effectiveness of cybersecurity risk management processes in all sectors and their impact on the communications sector.

E. Communications Sector Implementation Guidance Recommendations

The following recommendations address the Working Group 4 charge to provide the communications sector with guidance for implementing the NIST Cybersecurity Framework.

- CSRIC recommends that the FCC 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.
- CSRIC recommends that the FCC continue to collaborate with NIST and DHS in the further development of the NIST CSF and the promotion of programs to increase the voluntary use of the CSF.

- CSRIC recommends that the FCC partner with other departments and agencies to promote education and awareness of the cybersecurity risks inherent in critical communications infrastructures, and to promote steps that the communications sector can take to give external stakeholders with macro-level assurance that these collective actions are successfully managing cybersecurity risks.
- CSRIC recommends the FCC 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.
- CSRIC recommends the FCC 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.

VIII. ACKNOWLEDGEMENTS

Working Group 4 would like to acknowledge the significant contributions of each of its members, for without their expertise, participation, analysis, and contributions throughout the process, the report findings, conclusions, and recommendations contained herein would not have been possible.

Working Group 4 would also like to acknowledge the segment and feeder subgroup leadership team, comprised of Kelly Williams, Matt Tooley, John Marinho, Chris Boyer, Donna Bethea Murphy, Harold Salters, Larry Clinton, Susan Joseph, Jesse Ward, Russell Eubanks, Joe Viens, Tom Soroka, Brian Scarpelli, and Chris Roosenraad, who led their teams in conducting the segment and feeder analyses upon which the report's findings, conclusions, and recommendations are based.

Working Group 4 would also like to acknowledge the Working Group's advisors, Donna Dodson, Lisa Carnahan, Tony Sager, and Emily Talaga, for their expertise, thoughtful advice, and encouragement throughout the process.

Working Group 4 would also like to acknowledge the FCC liaison to the Working Group, Vern Mosley, for his substantial support and contributions throughout the process.

Working Group 4 would also like to acknowledge Matt Tooley for his administration of the Working Group's box.com account that the Working Group used to collaborate in sharing information among the Working Group members and in producing the report.

Working Group 4 would also like to thank Robert Mayer, Pat Murray, Deontrea Campbell, and the many other USTelecom support staff members for hosting the Working Group 4 face-to-face meetings. The Working Group greatly appreciates the significant planning and logistics that went into hosting the many successful face-to-face meetings.

Working Group 4 would also like to acknowledge the skilled expertise and dedication of the Final Report drafting team comprised of Paul Diamond, Stacy Hartman, Robert Thornberry, Brian Allen, Robert Mayer, and the segment and feeder subgroup leadership team. Without their perseverance and attention to detail, the Final Report would not have been possible.

And last but certainly not least, the Working Group 4 members would like to acknowledge and thank our esteemed Working Group 4 co-chairs, Robert Mayer and Brian Allen. Their insight, focus, expertise, outreach across the communications sector, and leadership throughout the process is evidenced by the quality of the Final Report's findings, conclusions, and recommendations.

IX. REPORTS & SEGMENTS

9.1 BROADCAST SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY

The Broadcast Industry Segment subgroup of Working Group 4 (WG4) focused on developing recommendations that will assist in reducing cybersecurity risk to broadcast critical on-air operations through the application of the NIST Cybersecurity Framework (NIST CSF).

To accomplish this objective the Broadcast Segment Group's mission was to provide a roadmap for broadcasters to align their specific operations to that of the NIST Cybersecurity Framework. While the NIST Framework may be used beyond critical infrastructure, the analysis was primarily focused on critical infrastructure as defined in the Cybersecurity Executive Order. For broadcasters, this means maintaining on-air operations in order to deliver news, weather, critical public warning, and emergency information to the communities that they serve. Broadcasters do not provide Internet Protocol (IP) network services to others but acquire them from IP service providers. However, broadcasters' critical on-air operations are enabled by IP networks and have in recent years become more and more dependent upon them. Individual broadcast companies should consider utilizing the steps outlined in this report to update or develop their own cyber risk management programs, applying the framework to their own unique circumstances.

II. INTRODUCTION

The Broadcast Segment is a subgroup within CSRIC IV Working Group 4 focused on developing recommendations that will assist in reducing cybersecurity risk to broadcast on-air operations through the application of the NIST Cybersecurity Framework (CSF).

The scale of the broadcast industry is fairly unique among the other communications industry segments. The broadcast industry is diverse, more than 15,000 radio and 1,700 television broadcasting facilities in the United States, providing news, emergency information and other programming services free, over the air to consumers. While many of these operations are broadcast networks and group owed, individual licensees tend to be small to medium sized operations, with relatively limited Information Technology (IT) support.

The broadcast industry is increasingly characterized by a reliance on the Internet and other IP based infrastructure for its core on-air operations. For the past several years, the broadcast industry has been transformed by a transition to file-based workflows and increased focused on IP networking and content delivery. A number of broadcasters continue to expand their reliance on central casting – concentrating on-air operations in regional hubs. Also growing rapidly is the use of "cloud-based" services by broadcasters, particularly in the areas of streaming, archiving, editing, transcoding, and content distribution.

In 2012 the Communications Sector, in partnership with the Department of Homeland Security (DHS), completed the 2012 Risk Assessment for Communications (referred to going forward as the National Sector Risk Assessment or NSRA), updating its 2008 report ,which assessed physical and cyber threats to the communications infrastructure. The risk assessment was intended to further the goals of the Communications Sector Specific Plan, also developed jointly

with DHS in 2010, to identify and protect national critical infrastructure, ensure overall network reliability, maintain "always-on" service for critical customers and quickly restore critical communications functions and services following a disruption.

In order to accomplish the foundational objectives established by the FCC for CSRIC IV WG4, the Broadcast Segment group sought to develop recommendations which will enable the NIST Cybersecurity Framework to be conformed in such a way that that it may be used by the broadcast industry to assess the vulnerability of critical on-air operations in the context of critical infrastructure as defined in the Cybersecurity Executive Order[38] and the NSRA. Please note this report does not address security of the Emergency Alert System (EAS) and its associated ecosystem. EAS security is considered in CSRIC IV Working Group III.[39]

III. BROADCAST SEGMENT GROUP MEMBERS

Member	Company
Adrienne Abbott	Nevada Association of Broadcasters
Sohail Anwar	National Public Radio
Edward Czarnecki	Monroe Electronics, Inc. / Digital Alert Systems
Seton Droppers	Public Broadcasting System
Christopher Homer	Public Broadcasting Service
Robert Ross	CBS Television Network
David Williams	National Public Radio
Kelly Williams	National Association of Broadcasters

IV. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objective

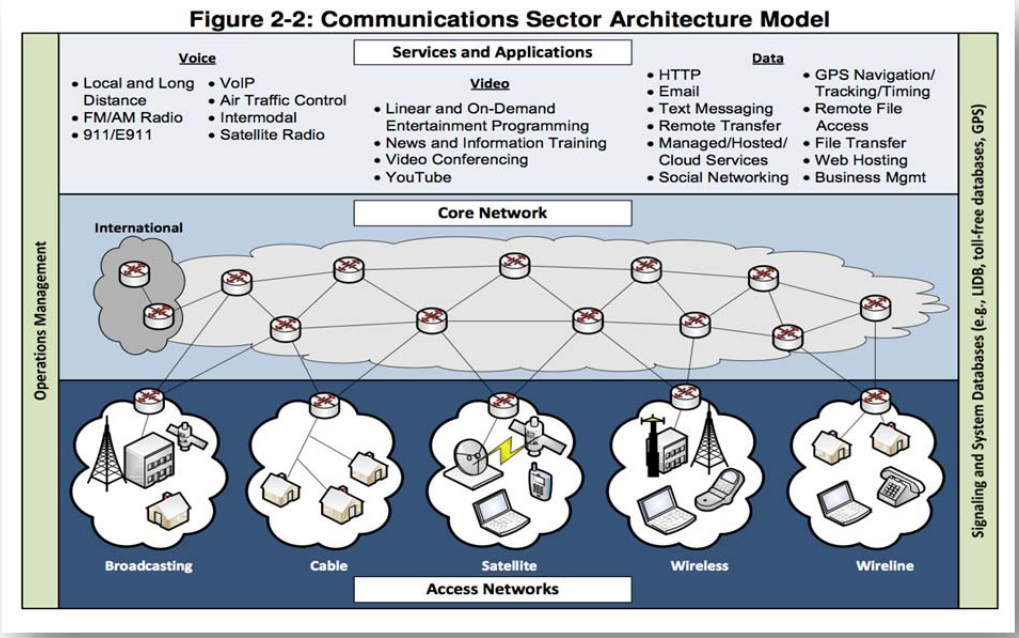
CSRIC IV WG4 was tasked with developing voluntary mechanisms that provide macro-level assurance to the Federal Communications Commission (FCC) and the public that communication providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise. WG4 also was charged with providing implementation guidance to facilitate the use and adaptation of the voluntary NIST Cybersecurity Framework (CSF) by communications providers. Consistent with Working Group 4's larger objective, the broadcast segment group analyzed the NIST Cybersecurity Framework version 1.0 from the perspective of the broadcast industry in order to apply the practices and processes described therein to this segment of the communications sector.

[38] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013) [hereinafter *EO 13636*].

[39] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council III, *Working Group 3 Emergency Alert System (EAS) – Initial Report CSRIC WG3 EAS Security Subcommittee Report (*2014), *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf.

B. Scope

Based on the NIST cybersecurity framework in critical infrastructure, the broadcast segment group focused on identifying the aspects of the broadcast infrastructure that would be considered critical infrastructure supporting the critical services broadcasters provide. Based on the definitions of critical infrastructure outlined in the NSRA and Executive Order 13636, the group concluded that it is broadcaster's role in public alerting and as "first informers" (i.e. keeping the public informed during time of emergency) that fulfils this critical infrastructure role. The NSRA communications architecture model illustrating what is considered critical infrastructure is shown below.

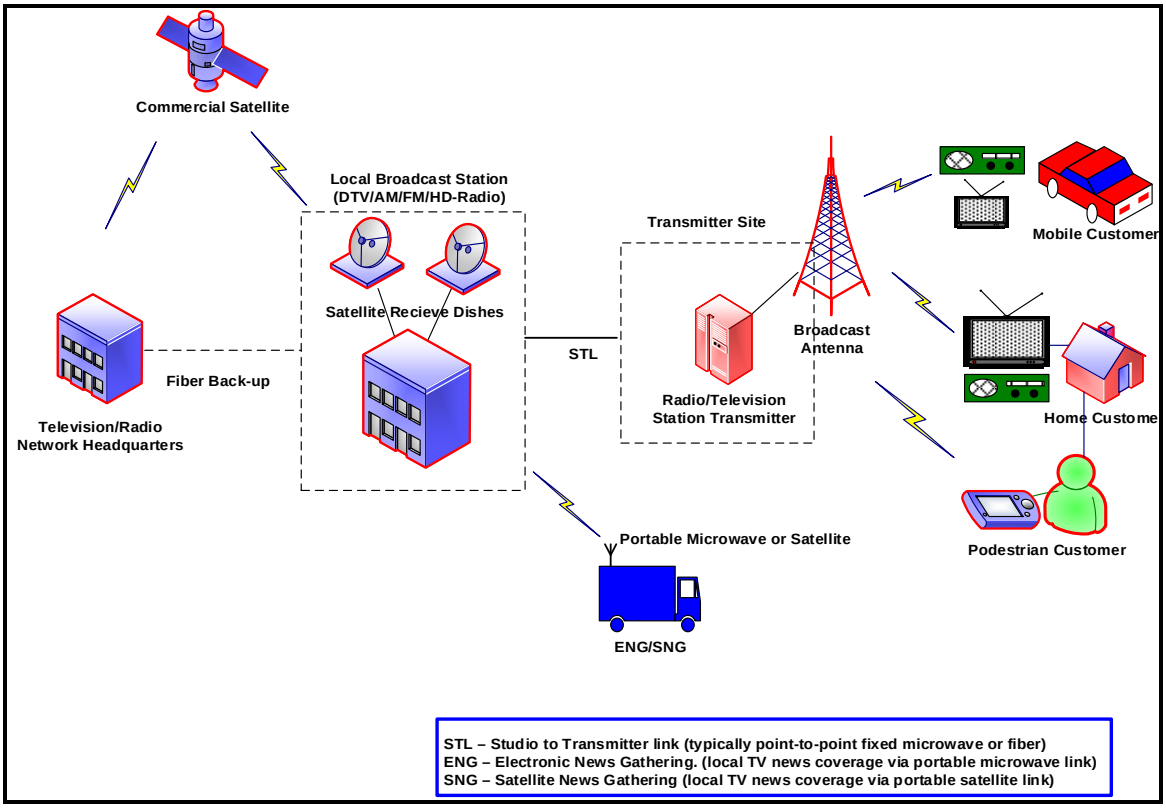


The broadcast segment group agreed with the other Segment groups that the scope of its efforts should build upon the work already completed in the NSRA, which is to "… ensure overall network reliability, maintain "always-on" service for critical customers and quickly restore critical communications functions and services following a disruption." Considering all these factors the Broadcast Sector group concluded that maintaining the on-air operations at local, regional and national level was constituted maintaining this segment of the national critical communications infrastructure.

It is important to note that Broadcasters are consumers of IP based network services and do not supply IP services to others, as such, they must evaluate the risk and vulnerability of their assets in the context on maintaining their critical on-air operations.

C. Methodology

Starting with the Broadcast architecture model from the NSRA (below), the broadcast segment analyzed the broadcast ecosystems and developed four architecture models that are illustrative of the different types of operations in the broadcast segment - Local Broadcast Station, Small Radio Station, Hubbed (or Central Cast) Operation, and Broadcast Program Network. These models, described in more detail in Section V, can help broadcasters identify the critical assets that may require different approaches to application of the NIST Framework. These critical elements delineate the scope of assets intended to be protected through the further analysis below.



V. RESULTS AND FINDINGS

A. Critical Services

The broadcast segment utilized the NIST cybersecurity framework to evaluate its application to the broadcast sector. Since the broadcast sector provides a service to consumers by providing news, weather and emergency information through over-the-air signals or, in the case of a program network, via satellite or leased fiber facility, many of the cyber security concerns may not appear to be applicable.

After careful review, the broadcast segment determined that there are aspects of broadcasting infrastructure that are IP network based and critical to providing essential services. Broadcasters are used to carrying mission critical data and information. Broadcasters must assess which parts of their infrastructure are critical to maintaining on-air operations so that they can deliver the following types of essential information to the public.

1) Emergency Alert Systems (EAS)

New technology in emergency alerting now carry messages from the Federal Emergency Management Association (FEMA) through IP networks using Common Alerting Protocol (CAP). Many state and local emergency management organizations have also adopted CAP protocol messaging distributed via IP over dedicated or public internet. The broadcaster's IP networks that carry these critical messages need to be protected against cyber-attacks[40].

2) News and Weather and Other Emergency Information

Broadcast stations and networks provide essential content in the form of news and weather and other emergency information, such as evacuation routes or tornado tracking. Both information and content flow over high speed IP networks within a broadcast plant to provide integration of News Room Computer Systems (NRCS), audio and video servers, graphics systems and scheduling/automation systems. The broadcast network is the "backbone" of the station or network and needs to be carefully managed for redundancy, reliability and security. Important feeds and wire services that are used to solely rely on satellite or microwave have also migrated go IP and Long-Term Evolution (LTE) networks in order to provide valuable and timely content.

B. Broadcast Ecosystem Architectures

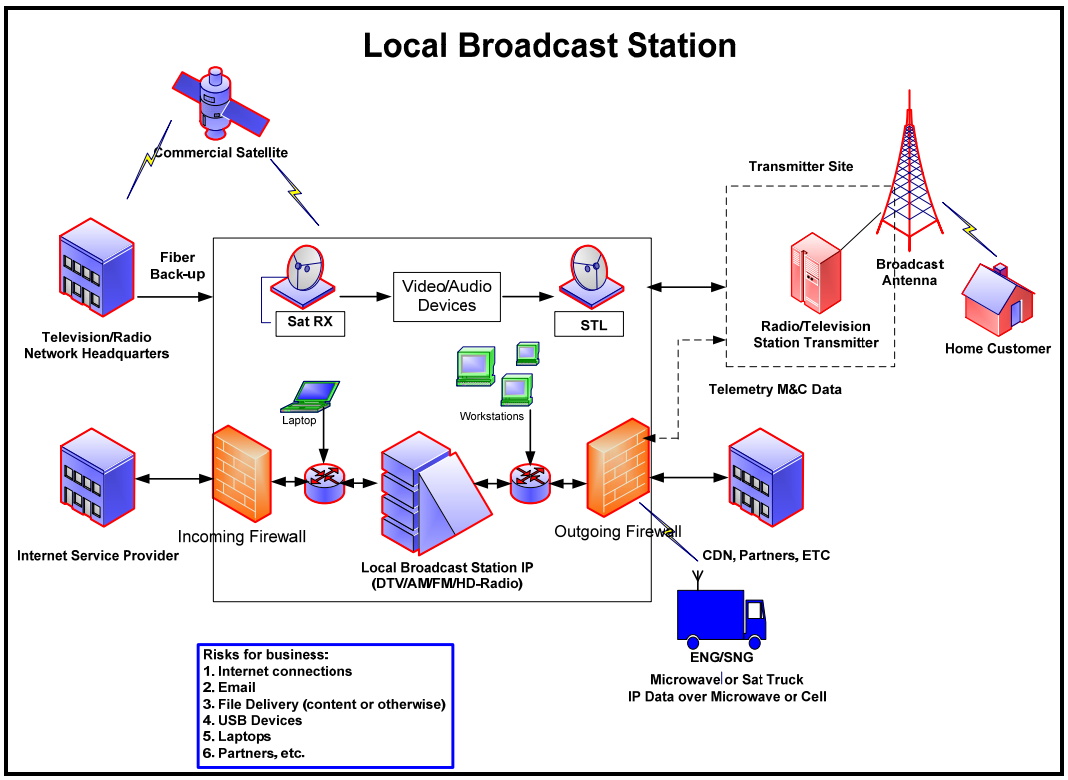
Below are the four architecture models that are illustrative of the different types of operations in the broadcast segment. Broadcasters can use the model that most closely

[40] This report does not address specifics of security for EAS and its associated ecosystem. EAS security is considered in CSRIC Working Group III.

resembles their actual infrastructure to identify the assets that require threat analysis and evaluation when applying the framework to on-air operations

1) Local Broadcast Station

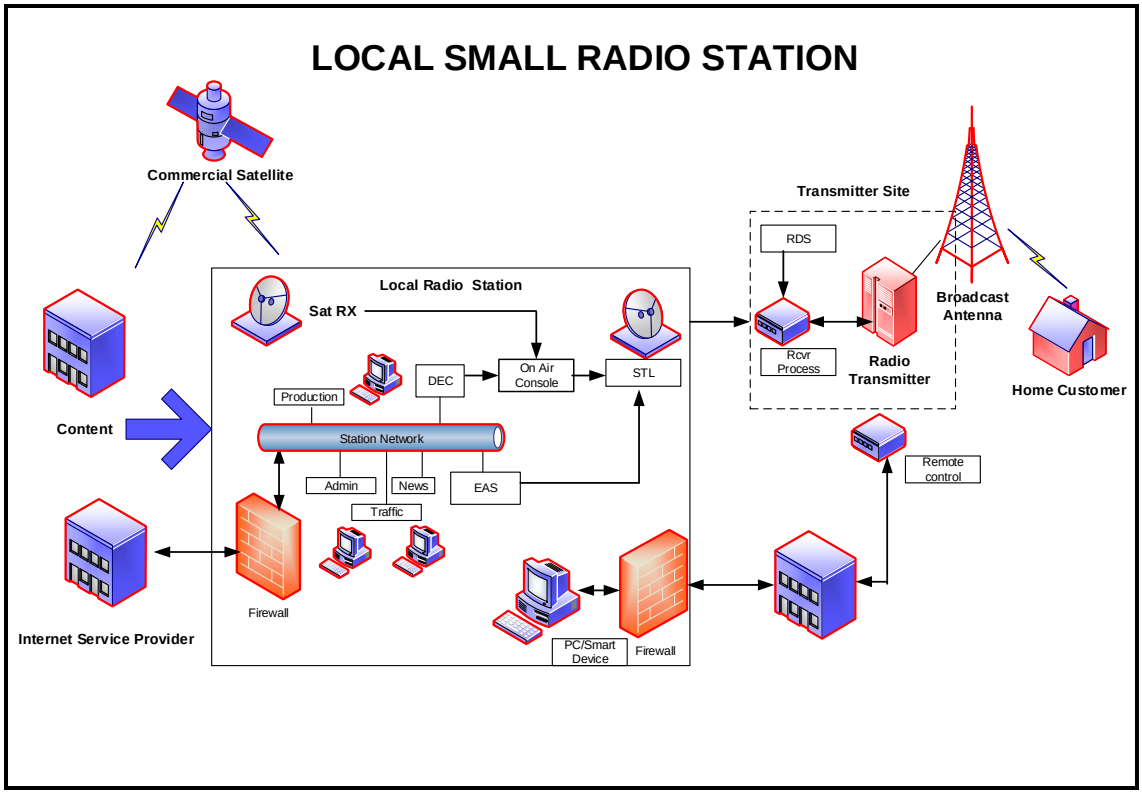
Broadcast stations include independent, public, educational or state, station groups or network O&O's (owned and operated). A broadcast station can be a handful of employees in a "mom and pop" shop to major market stations with hundreds of employees. Many functional areas within a station include but are not limited to sales, programming, traffic, production, news, community affairs, public relations, accounting and finance, and engineering and operations. Engineering and Operations typically operates on a 24X7 basis a plays a critical role in providing content for community service, news, weather, sports, and entertainment for their broadcast market.



2) Local Small Radio Station

Local Radio Stations may not have enterprise level networks as larger broadcasters do, but there are many areas where the station network connectivity provides critical services to its audience and would necessitate cyber security measures. This includes programming source(s) delivered via IP, commercial delivery and commercial production, other production resources such as Associated Press (A/P) news wire service delivery, remote operations, Common Alerting Protocol (CAP)/EAS Internet access, and Studio Transmitter Links (STL) transmitter metering and control. The network could also be used to provide for transmitter site security A/P news, station

social Media/applications/contests/games, in-house Wi-Fi access, FCC accounts, Traffic Bookkeeping (includes staff and listener accounts), and portable media using Universal Serial Bus (USB) or Bluetooth.



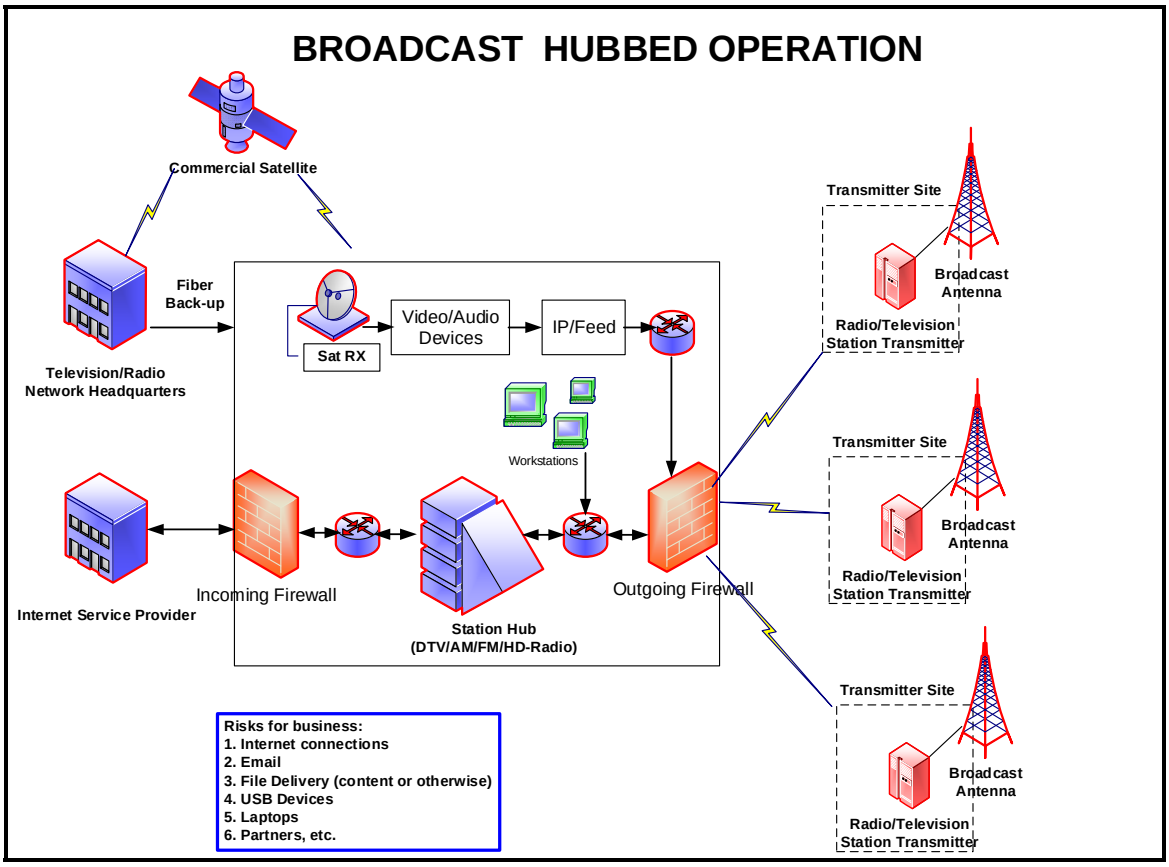
3) Broadcast Hubbed (Central Cast) Operation

Broadcast station hub is somewhat different from a broadcast station. A broadcast station typically takes the repetitive 24X7 master control operations of two or more broadcast stations and combines them into a single facility for efficiency purposes. These can include private third party business, educational or state, station groups or network O&O's (owned and operated) hubs. A television station that is a spoke of a hub facility does not need to be a small market facility. A hubbed television station is a fully featured and functioning facility that can have a news department, promotions, and be a network affiliate or independent. It simply does not have a master control facility to originate its programming to the local broadcast transmitter. There are two ways to accomplish this:

- The central hub originates all content which is sent to the satellite station as a video stream over a private bandwidth circuit. Local commercials, news programming, and other interstitial material are sent in the other direction to the hub for transmission at a later time or in real time in the case of live news programming. Traffic operations are also usually centralized at the hub facility., or

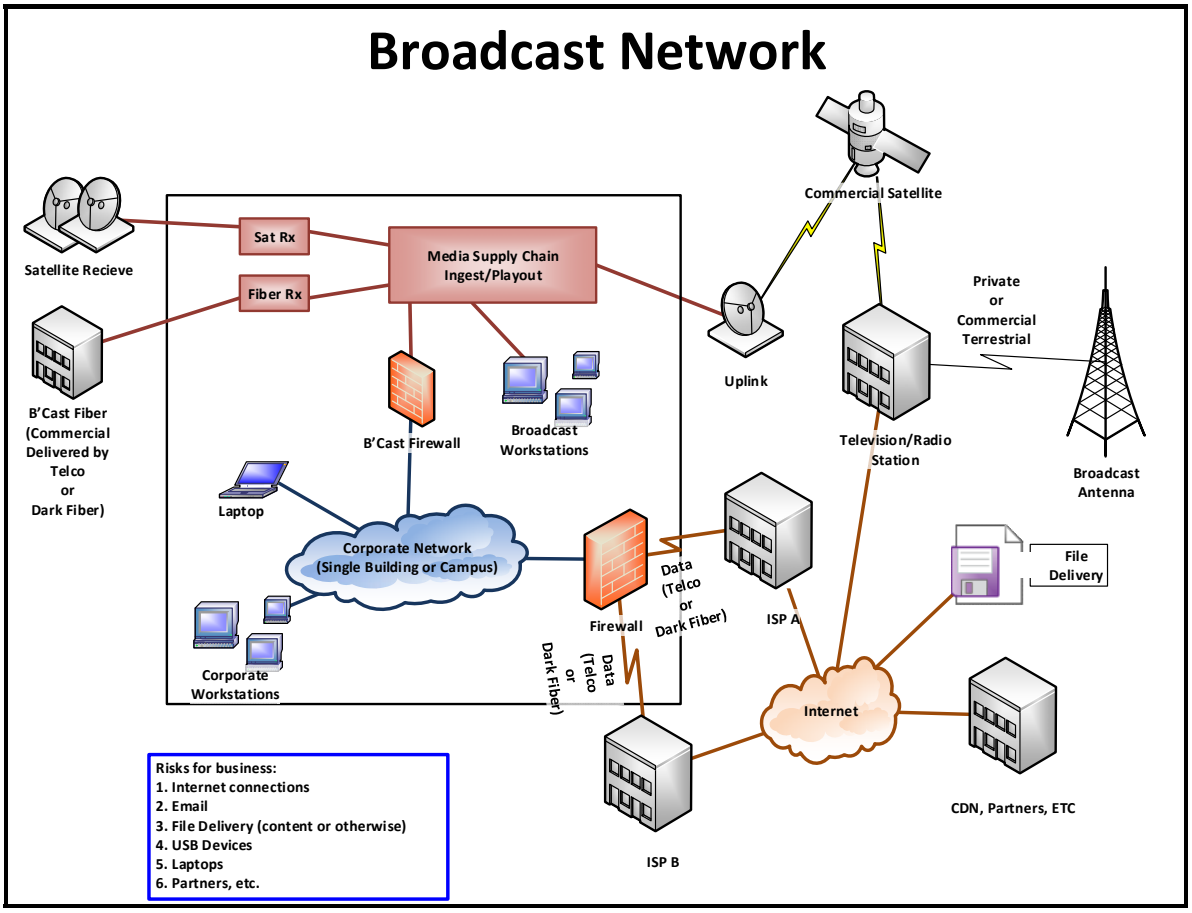
- The satellite station has all of the content material and equipment onsite, but is controlled from the central hub.

Today with the cost of bandwidth being much lower than five years ago most central-casting locations use method number one. The obvious security and redundancy issues regarding protection of the feed from the hub require that two diverse routes should be employed with firewalls and VPN protection. All other data circuits, computers, digital streaming feeds, feeds of any type should be protected as they would be in any other modern broadcast facility.



4) Broadcast Network

Broadcast networks provide content to stations, cable companies, satellite providers and even OTT (Over the Top) broadcast. A broadcast network range from a few hundred to a few thousand employees and typically provides a national or international footprint for distribution. Many functional areas within a network include, but are not limited to, sales, programming, traffic, production, news, public relations, accounting and finance, and engineering and operations. Engineering and Operations typically operates on a 24X7 basis a plays a critical role in providing content for stations, cable companies, satellite providers and OTT distributors. This content eventually makes its way to the public for news, sports, weather, education, public interest, and entertainment.



VI. APPLYING THE NIST CYBERSECURITY FRAMEWORK

The NIST Framework presents five Core Functions organizations can use to evaluate their cybersecurity risks.

- **Identify** – *Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.* The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

- **Protect** – *Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.* The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – *Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.* The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – *Develop and implement the appropriate activities to take action regarding a detected cybersecurity event*. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – *Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event*. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

VII. APPLICATION METHODOLOGY

The CSRIC IV Broadcast Sub-Committee reviewed the NIST framework as it applies to the different segments of the broadcast industry;

- Small Radio Station
- Local Broadcast Station
- Station Hub (or Central Cast) Operation
- Broadcast Network

Each of the 98 sub-categories of the NIST Framework were evaluated as to being non-critical, may be critical, or critical for each of the types of broadcast infrastructure models. This helps define how the scope of the framework can be applied to broadcast organizations of differentiating scope and size.

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

ID.BE-4: Dependencies and critical functions for delivery of critical services are established		May be Critical	Critical	Critical
ID.BE-5: Resilience requirements to support delivery of critical services are established		May be Critical	Critical	Critical
ID.GV-1: Organizational information security policy is established			May be Critical	May be Critical
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners			Critical	Critical
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	May be Critical	May be Critical	Critical	Critical
ID.GV-4: Governance and risk management processes address cybersecurity risks	Critical	Critical	Critical	Critical
ID.RA-1: Asset vulnerabilities are identified and documented	Critical	Critical	Critical	Critical
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	May be Critical	May be Critical	Critical	Critical
ID.RA-3: Threats, both internal and external, are identified and documented	Critical	Critical	Critical	Critical
ID.RA-4: Potential business impacts and likelihoods are identified	May be Critical	May be Critical	Critical	Critical
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Critical	Critical	Critical	Critical

ID.RA-6: Risk responses are identified and prioritized	Critical	Critical	Critical	Critical
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	May be Critical	May be Critical	Critical	Critical
ID.RM-2: Organizational risk tolerance is determined and clearly expressed			Critical	Critical
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis			May be Critical	May be Critical
PR.AC-1: Identities and credentials are managed for authorized devices and users	Critical	Critical	Critical	Critical
PR.AC-2: Physical access to assets is managed and protected	Critical	Critical	Critical	Critical
PR.AC-3: Remote access is managed	Critical	Critical	Critical	Critical
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Critical	Critical	Critical	Critical
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	Critical	Critical	Critical	Critical
PR.AT-1: All users are informed and trained	May be Critical	May be Critical	Critical	Critical

PR.AT-2: Privileged users understand roles & responsibilities	Critical	Critical	Critical	Critical
PR.AT-3: Third-party stakeholders (e.g., suppliers customers, partners) understand roles & responsibilities	May be Critical	May be Critical	May be Critical	May be Critical
PR.AT-4: Senior executives understand roles & responsibilities	May be Critical	May be Critical	Critical	Critical
PR.AT-5: Physical and information security personnel understand roles and responsibility	Critical	Critical	Critical	Critical
PR.DS-1: Data-at-rest is protected	Critical	Critical	Critical	Critical
PR.DS-2: Data-in-transit is protected	Critical	Critical	Critical	Critical
PR.DS-3: Assets are formally managed throughout removal, transfers and disposition			Critical	Critical
PR.DS-4: Adequate capacity to ensure availability is maintained			May be Critical	May be Critical
PR.DS-5: Protections against data leaks are implemented	May be Critical	May be Critical	Critical	Critical
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Critical	Critical	Critical	Critical

PR.DS-7: The development and testing environment(s) are separate from the production environment			Critical	Critical
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained			Critical	Critical
PR.IP-2: A System Development Life Cycle to manage systems is implemented			May be Critical	May be Critical
PR.IP-3: Configuration change control processes are in place	Critical	Critical	Critical	Critical
PR.IP-4: Backups of information are conducted, maintained and tested periodically	Critical	Critical	Critical	Critical
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met			Critical	Critical
PR.IP-6: Data is destroyed according to policy			May be Critical	May be Critical
PR.IP-7: Protection processes are continuously improved	May be Critical	May be Critical	Critical	Critical
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	May be Critical	May be Critical	Critical	Critical
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Critical	Critical	Critical	Critical

PR.IP-10: Response and recovery plans are tested	May be Critical	May be Critical	Critical	Critical
PR.IP-11: Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening)	May be Critical	May be Critical	Critical	Critical
PR.IP-12: A vulnerability management plan is developed and implemented			May be Critical	May be Critical
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools			May be Critical	May be Critical
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	Critical	Critical	Critical	Critical
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy			May be Critical	May be Critical
PR.PT-2: Removable media is protected and its use restricted according to policy	May be Critical	May be Critical	Critical	Critical
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Critical	Critical	Critical	Critical
PR.PT-4: Communications and control networks are protected	Critical	Critical	Critical	Critical
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed			May be Critical	May be Critical

DE.AE-2: Detected events are analyzed to understand attack targets and methods	May be Critical	May be Critical	Critical	Critical
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors			Critical	Critical
DE.AE-4: Impact of events is determined	May be Critical	May be Critical	Critical	Critical
DE.AE-5: Incident alert thresholds are established	May be Critical	May be Critical	Critical	Critical
DE.CM-1: The network is monitored to detect potential cybersecurity events	Critical	Critical	Critical	Critical
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Critical	Critical	Critical	Critical
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	May be Critical	May be Critical	Critical	Critical
DE.CM-4: Malicious code is detected	Critical	Critical	Critical	Critical
DE.CM-5: Unauthorized mobile code is detected	Critical	Critical	Critical	Critical
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Critical	Critical	May be Critical	May be Critical

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	May be Critical	May be Critical	Critical	Critical
DE.CM-8: Vulnerability scans are performed	May be Critical	May be Critical	Critical	Critical
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability			May be Critical	May be Critical
DE.DP-2: Detection activities comply with applicable requirements			May be Critical	May be Critical
DE.DP-3: Detection processes are tested	May be Critical	May be Critical	May be Critical	May be Critical
DE.DP-4: Event detection information is communicated to appropriate parties	May be Critical	May be Critical	Critical	Critical
DE.DP-6: Detection processes are continuously improved	May be Critical	May be Critical	Critical	Critical
RS.RP-1: Response plan is executed during or after an event	Critical	Critical	Critical	Critical
RS.CO-1: Personnel know their roles and order of operations when a response is needed	Critical	Critical	Critical	Critical
RS.CO-2: Events are reported consistent with established criteria	Critical	Critical	May be Critical	May be Critical

RS.CO-3: Information is shared consistent with response plans			May be Critical	May be Critical
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Critical	Critical	Critical	Critical
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness			May be Critical	May be Critical
RS.AN-1: Notifications from detection systems are investigated	Critical	Critical	Critical	Critical
RS.AN-2: The impact of the incident is understood	May be Critical	May be Critical	Critical	Critical
RS.AN-3: Forensics are performed			Critical	Critical
RS.AN-4: Incidents are categorized consistent with plans			Critical	Critical
RS.MI-1: Incidents are contained	Critical	Critical	Critical	Critical
RS.MI-2: Incidents are mitigated	Critical	Critical	Critical	Critical
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Critical	Critical	Critical	Critical
RS.IM-1: Response plans incorporate lessons learned			Critical	Critical

RS.IM-2: Response strategies are updated			May be Critical	May be Critical
RC.RP-1: Recovery plan is executed during or after an event	May be Critical	May be Critical	Critical	Critical
RC.RP-1: Recovery plans incorporate lessons learned			Critical	Critical
RC.RP-2: Recovery strategies are updated	May be Critical	May be Critical	Critical	Critical
RC.CO-1: Public related are managed	May be Critical	May be Critical	May be Critical	Critical
RC.CO-2: Reputation after an event is repaired				
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams			May be Critical	May be Critical

VIII. ILLUSTRATIVE USE CASES

Cyber security involves all broadcast stations regardless of size. As a broadcaster you may think there is no real potential risk to your business from cyber security attacks since your business simply puts news and entertainment over the airways.

But, consider how many stations have a web presence and are now streaming the morning news and traffic reports. And that many stations have sophisticated financial system so folks on the road can access everything from the viewer database to sales tools. In engineering, just about everything has an internet connection now (e.g., the EAS system is directly connected to FEMA and National Weather Service for Emergency Alerts).

The NIST Framework can help make sense of potential cyber security risks for stations going down this road for the first time. The first step is to take a look at the new cyber security framework and make it a part of your business. There are many resources available and technical expertise can be either your internal IT department or an external cyber security specialist.

As a local radio or television broadcaster you have a commitment to your community for which you are licensed. Making cyber security part of your business protects your revenue, your employees, your viewers, and your community at large. The best way to get started is start small and identify what needs to be protected first.

1) What are you trying to protect?

If you have a news organization there are many systems that are vulnerable for attack. These include but are not limited to; news room computer system, playout servers and automation, graphics machines, news reporters' laptops, and cellular devices used to bring stories in from the field. A firewall is good but cannot protect from bad practices such as not providing controls on network access, unprotected laptops, and "thumb" drives introduced to the network and employees visiting untrusted web sites.

2) Who is responsible/involved in the process?

Cyber security isn't someone else's job, it is everyone's job. Support from all stakeholders is the key to success. The support for cyber security needs must start at the leadership level and everyone from the General Manager, Programming, News Director, Sales Manager, HR, IT, and Engineering needs to understand and support these efforts.

3) How do you tackle the Framework? What do you do first?

Once the station leaders support the initiative, bring together the stakeholders and provide the guidance and education regarding what is involved and what each individual's roles and responsibilities are. You may find once people are educated there will be better understanding of the process (such as taking systems down to install latest security patches). Cyber security can be made to fit any culture.

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

Review the framework and focus on what is most important to protect your "critical" systems and work out from there. Businesses can approach the framework in many ways. It doesn't matter if the easy stuff goes first or if the more critical does, but doing nothing is not an option.

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

Once you get through all the initial items on the cyber security framework you may find the more you move into to it, the easier it gets. You can then even start on some of the items from the "big guys" to help your continuous improvement process. You may still get groans from the reporters when you make sure their machine is scanned before they can get on the network - but they at least now will know the importance of good

cyber security. Proper cyber security can work for all businesses and the framework can provide the roadmap.

A. Broadcast Radio/TV Station/Hub Assessment

1) Internet Access- In a fast paced operation where both resources and time are scarce, there is a need to ensure proper security protocols are communicated and followed on a regular basis. In this case, employees are aware of the company's goals and strategy for security, employees are trained and operating procedures and protocols are established and communicated. Examples of this could include use of only "trusted" internet sites, a well-established email policy to ensure employees avoid opening email from "unknown" sources, and discipline in using company and personal resources. This is defined in the analytical framework in several areas;

    - Risk Management Strategy
    - Awareness and Training
    - Communication

2) File/Content Delivery-Broadcasting is moving towards a more IP based infrastructure where videotape content is being replaced with file based content. These files are large in size and may require special high speed networks and high throughput storage systems. Security measures need to be in place without impeding the timely workflow process required to receive large content files. These files can be delivered through networks, hard drives or even USB type devices. Many of the files are in a proprietary format (e.g., Apple Pro Res, AVID DNX, etc.) and require special security measures. Network delivery systems such as Signiant and Aspera provide the user a path to implement a security layer. This is defined in the analytical framework in the following areas;

    - Protective Technology
    - Detection Process
    - Continuous Monitoring
    - Mitigation

3) News and Production - News and production have unique challenges in security. Many of the policies described in "Internet Access" would be included, but there may be many instances where going outside "trusted" sources may be required to obtain "news worthy" information. Also, microwave technology for backhaul of "live" shots is quickly being replaced with new technology such as "bonded LTE" to provide "live" or file-based content for news, sports or other programming. Another unique challenge is much of the personnel are often not full time employees, but contract workers, per diem production staff and "stringers" (such as photographers and camera operators). Providing the proper training and discipline may be difficult

and require careful vetting and clear and easy to understand expectations and procedures. This is defined in the analytical framework in several areas;

- Risk Management Strategy
- Awareness and Training
- Communication
- Information Protection Processes and Procedures

4) Partners - Without the cooperation of key business partners' security measures may be difficult to administer even within the most disciplined organizations. Broadcast organizations rely on network providers, satellite providers, equipment providers and service providers to ensure all security measures are in place. Unfortunately much of the legacy broadcast equipment still in use does not support security patching, auto updating, or system monitoring through configuration management databases (CMDB) and other controls. It is recommended that broadcast organizations address this by making security an integral part of the requirements for purchasing new equipment and services. This is defined in the analytical framework in the following areas;

- Asset Management
- Risk Management
- Continuous Monitoring
- Detection Processes

Regarding hubbed operations, the obvious security and redundancy issues regarding protection of the feed from the hub require that two diverse routes should be employed with firewalls and VPN protection. All other data circuits, computers, digital streaming feeds, feeds of any type should be protected as they would be in any other modern broadcast facility (see stations above). The best way to accomplish is to work closely with your vendor and security experts. It may be better if they are not the same company so there are proper checks and balances.

Also ensure everyone involved understands their roles and responsibilities. Make sure incidents and changes are properly logged and documented. There should always be a back out plan for major changes that have an adverse effect. Many systems should have a test lab to try new software and hardware before it is deployed, but this may not be possible in a large scale network that cannot be replicated. Put together a response plan and track recovery time for continuous improvement.

While a hubbed infrastructure provides efficiencies in a multi-station operation it is important to recognize that there is an increased risk which may impact the ability to provide essential and important services to listeners and viewers in multiple markets.

B. Broadcast Networks - Broadcast Firewall

As a Network Broadcaster Engineering Manager you have an obligation to the stations that depend on your distribution of content, including content for public interest and emergency information. There are many legacy broadcast systems that are not protected from cyber security attacks, monitored for threats nor properly controlled.

Many IT groups have the necessary talent within their security staff to help identify the risks and create a plan to help mitigate them. It is important to gain support from your leadership including Technology Officer, Administrative, Programming, and Finance before you review and then use the NIST Cybersecurity Framework to protect core network and critical infrastructure used in Broadcast Operations.

The areas that should be focused on are access points to our critical production, ingest and broadcast systems. This involves possibly installing inbound/outbound firewall at all campuses. This broadcast demilitarized zone (DMZ) separates the broadcast Local Area Network (LAN) from the administration LAN, and provides the necessary protection. As a group, you should review the categories within the NIST Framework, and based upon your initial risk assessment focus on what has the greatest urgency to implement within your broadcast network**.** Then devise a plan for a review and recommendation on the following categories: (1) identify, (2) detect, (3) protect, (4) respond, and (5) recover.

Once you complete your analysis the next step is implementation. This is not as easy as one would imagine since many of the systems involved may never have had a firewall or constraints (such as virus protection, etc.), so the approach is to proceed cautiously and carefully:

1. Access Control - New Firewalls may need to be installed without restrictions so a full audit and analysis could be completed before making changes.
2. Data Security - A strict change management process should be instituted so any new Firewall rules could be quickly backed out if needed.
3. Information Protection & Process Improvement - A communication plan should be devised to ensure all stakeholders were informed of the risks.
4. Anomalies & Events- The network should be continuously monitored to detect potential cybersecurity events.

As you can see it is not only important to place cyber security controls within the network, but to collaborate within groups go ensure success. It is also recommended to have regular meetings with your new “cyber security committee” and meet regularly to discuss the latest threats, changes to our security protocols, and next step for implementing the framework. Each quarter you should review the NIST Framework against your business and look for new ways to improve our systems and processes.

IX. CONCLUSIONS AND RECOMMENDATIONS

- Broadcasters are not providers of IP networks but are consumers of these services and delivery of critical news and public warning services are enabled these networks.

- Periodic assessment and understanding of potential cyber threats to broadcasters' IP infrastructure is essential to maintaining their critical on-air operations.

- Broadcast industry organizations should review this report and use the risk management matrix above and the analytical process outlined herein to adapt the NIST Framework approach as appropriate to cybersecurity risk management in a manner that best fits their own operations and infrastructure.

- No new regulations are warranted to address conformity to the NIST Framework to the broadcast ecosystem. The FCC should avoid taking a checklist approach to cybersecurity. Rather, broadcasters and their IP service providers are best positioned to understand their cybersecurity needs and risk tolerances, and should be afforded flexibility to apply the framework to their critical operations.

- The Broadcast industry is a diverse segment, consisting of large station groups and broadcast networks but also including many small entities. Thus continued flexibility is essential for use of the NIST Framework. Each broadcast entity is best positioned to understand and address its cybersecurity risks, and should be afforded flexibility to apply the framework to their specific architecture.

X. ACKNOWLEDGEMENTS

The broadcast segment acknowledges the substantial contributions of time and expertise from each of the individuals and companies represented on the subgroup.

9.2 CABLE SEGMENT CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4 March 2015

TABLE of CONTENTS

I. Introduction

The Cable Segment is a subgroup within CSRIC Working Group 4 focused on reducing cybersecurity risk to the cable network infrastructure through the application of the NIST Cybersecurity Framework (CSF). The last set of comprehensive cybersecurity best practices was recommended by CSRIC III WG2A in March 2011[41]. The Cable Segment evaluated CSRIC's existing cybersecurity best practices to determine how best to address alignment with the NIST Cybersecurity Framework.

II. Cable Segment Group Members

Member	Company
Bill Check	National Cable and Telecommunications Association
Bill Taub	Cablevision
Brian Allen	Time-Warner Cable
Charles Hudson	Comcast
Chris Roosenraad	Time-Warner Cable
John Kelly	Comcast
Jorge Nieves	Comcast
Joseph Viens	Time-Warner Cable
Mary Haynes	Charter Communications
Matt Tooley	National Cable and Telecommunications Association
Michael O'Reirdan	Comcast
Myna Soto	Comcast
Ramesh Sepehrrad	Comcast
Russell Eubanks	Cox Communications
Susan Joseph	CableLabs

III. Objective, Scope and Methodology

The foundational objectives of Working Group 4 include the following:[42]

- To conform the NIST framework to the communications sector. Identify core mission(s), critical infrastructure and risks to the communications sector and organize the NIST core framework based on the aspects most relevant to ensuring the reliability and integrity of the core communications infrastructure.

[41] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council II, *Working Group 2A Cybersecurity Best Practices – Final Report* (2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

[42] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management Best Practices (WG4)* (2014), *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-4_Report_061814.pdf.

- Maintain flexibility for individual companies. As part of this exercise, based on updated threat information, and consistent with the NIST framework, the communications sector conforming framework will allow for flexibility for individual companies to self-determine how to apply the framework to their business based upon their own individual risk profile, risk tolerance, and critical infrastructure ownership.

- Develop new streamlined practices that follow Framework organization and common risk management approaches. Use existing CSRIC Best Practices and other resources to inform and organize the Framework with the goal to provide companies a "guide" of practices specific to communication segments that companies could elect to implement to mitigate cyber risk.

- Develop use cases/examples of how the framework is being used within the sector. Develop an appendix with illustrative examples or use cases about how the framework is being used or incorporated into risk management processes of communications companies. Descriptions will be anonymized and provide examples for all sector members around how aspects of the framework could be voluntarily used in the communications sector.

- Provide guidance to incorporate framework into existing company risk management processes. Determine high level processes that companies could perform, to the extent they use the framework, to incorporate it into their existing risk management program, or build a cyber-risk management program where none exists today.

  The NIST Framework suggests seven steps for applying the Framework and, consistent with the FCC's charter for Working Group #4, allows for the framework to be tailored by individual companies to suit their unique needs characteristics, and risks. The steps include the following:

  1) **Prioritize and Scope**. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

  2) **Orient**. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

  3) **Create a Current Profile**. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

4) **Conduct a Risk Assessment**. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

5) **Create a Target Profile**. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

6) **Determine, Analyze, and Prioritize Gaps**. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities; supports risk management, and enables the organization to perform cost-effective, targeted improvements.

7) **Implement Action Plan**. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

Consistent with the other communications segments represented in this document, the cable segment took into account the seven steps suggested in the previously outlined NIST Framework, and examined how those steps apply and conform to the way that the cable industry is structured, and to how our networks operate. For the purposes of this report, we provide an example template that could be used as a guide to how members of the cable industry can apply the NIST Framework as a tool to mitigate threats to the cable critical infrastructure. Through the application of this holistic approach, operators can have a better understanding of both direct and indirect risks to their networks, how the cyber-threat vectors for those risks relate to supporting the overall functioning of critical communications, and create action plans to effectively protect against them.

For this report, the NIST Framework methodology has been used in the creation of a representative example that applies in a general way to the operation and business processes of a generic cable operator's network. Taking the form of a use case, the cable segment is offering an assessment template that can be modified and tailored to the needs of a given operator, and further developed into a full implementation plan that guides the organization in protecting and maintaining their critical assets. It must be stated that although cable networks have some commonality in their design, the organizational infrastructure and geographical distribution of assets varies widely. Therefore, the use case presented here assumes a centralized model that can be enforced in a top down approach, in a large organization with a clearly delineated hierarchical business structure. Those organizations with widely dispersed assets and relatively autonomous regional facilities should take into consideration their structure and apply the model accordingly.

For purposes of consistency with other sectors, the report is organized into two primary sections: (1) defining the methodology used by the cable segment group to prioritize the Framework best practices for cable critical infrastructure, which could also be used by cable segment members to address other issues depending upon their business needs; and (2) provide an illustrative example profile by applying that methodology to critical cable communications infrastructure.

To prioritize the NIST framework best practices the cable segment worked through a worksheet in collaboration with other segments (e.g. wireline, wireless) considering the best practices along a variety of factors. These include considering whether each functional area, category and sub-category were in or out of scope, how they may be applied, their criticality to protecting against cyber threats, and difficulty to implement. The working group also considered several barriers to entry including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers in assessing the degree of difficulty to implementing individual practices.

Finally the working group considered various threats from the Threats Feeder Group in conducting the criticality assessment. The results of this analysis were to categorize the various functional areas, categories and sub-categories into three buckets of practices between highest priorities, mid-tier and tertiary priority as outlined in Section IX of this document.

IV. Barriers to Participation

As noted above, the working group also considered several barriers to entry including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers in assessing the degree of difficulty to implementing individual practices. Please see the barriers sub-group report for a more detailed discussion of barriers associated with implementing framework.

V. Findings and Conclusions: Cable Segment

In order to create a sample profile, the cable segment first reviewed the NIST framework in the context of critical infrastructure. The framework could also be viewed for other factors beyond critical infrastructure consistent with each individual sector or company's priorities and core mission applying the seven steps outlined by NIST discussed above.

In developing a representative profile for critical infrastructure the segment considered critical infrastructure consistent with the definition discussed in President Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity" dated 12 February, 2013, critical infrastructure includes those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Further, in 2012 the Communications Sector, in partnership with DHS, completed the 2012 Risk Assessment for Communications (hereinafter the National Sector Risk Assessment or NSRA), updating its 2008 report, which assessed physical and cyber threats to the communications infrastructure. The risk assessment was intended to further the goals of the Communications Sector Specific Plan, also developed jointly with DHS in 2010, to identify and protect national critical network components, ensure overall network reliability, maintain "always-on" service for critical customers and quickly restore critical communications functions and services following a disruption. The cable segment agreed that the scope of the efforts in Working Group Four should build upon the work already completed in the 2012 risk assessment.

The NSRA assessed the risk to the communications infrastructure from both physical incidents and cyber-attacks. The results of this analysis concluded that while all cable network components are vulnerable to single incidents, the risks are limited to local—and not regional or national— disruptions and/or outages. The main risk area was determined to be third party support providers, submarine cable landing sites, long haul fiber optic cables, and core transport nodes that are vulnerable to malicious actors committing resource exhaustion – a threat that poses a substantial risk to national disruptions and/or outages.

Communications Sector Architectural Model

The NSRA proposes an architectural model that divides the communications network infrastructure into three components (1) services and applications, (2) core network and (3) access networks. The NSRA also combines the key communications features and services of the core networks into what is referred to as the "core network" and then identifies several service and application platforms such as voice, video and data.

The figure below from the 2012 NSRA illustrates the communications sector architectural model.

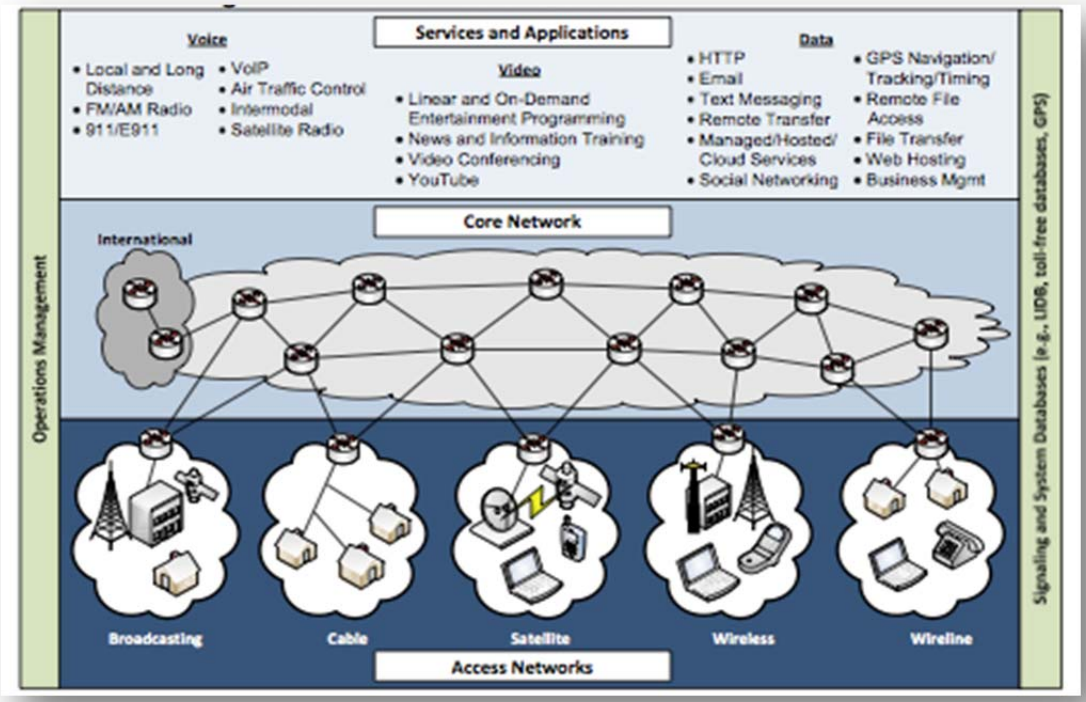


Figure 4 Communications Sector Architectural Model

The core network transports a high volume of aggregated traffic over large distances; typically via fiber or satellite and interconnects with access networks across the country. The core network is global, connecting all continents except Antarctica using submarine fiber optic cable systems and land-based fiber and copper facility networks. The converged core network uses various technologies for the physical (layer 1) and transport layers (layer 2) for the transport of the services.

Multiple service providers operating distinct core networks traversing the entire country provide the communications core infrastructure. These networks are primarily composed of wireline networks. The voice, video, and data services typically require some kind of routing translation query such as a host name look up or toll-free number query and are provided as part of operating the core network. In addition, the Network Operations Center (NOC), customer care centers, and data centers for all the access networks reside on the core network.

The access networks connect the end users to the core network. Traffic may originate and terminate with an access network without connecting to the core network.

A. Cable Networks

Cable networks are comprised of an access network and core network. Together these two networks form the cable network and also known as the Service Delivery Network (SDN) and are used to deliver voice, video, and data services including high-speed Internet access service.

B. Cable Access Networks

The cable access networks use a mixture of fiber and coaxial cable commonly referred to as hybrid fiber/coaxial (HFC) network to provide bi-directional signal paths to the customer. The HFC network effectively segments the cable system into a number of parallel distribution networks. Typically, HFC networks use a three-level topology (as shown in the figure below): 1) headend(s), 2) distribution hubs, and 3) multiple fiber nodes.

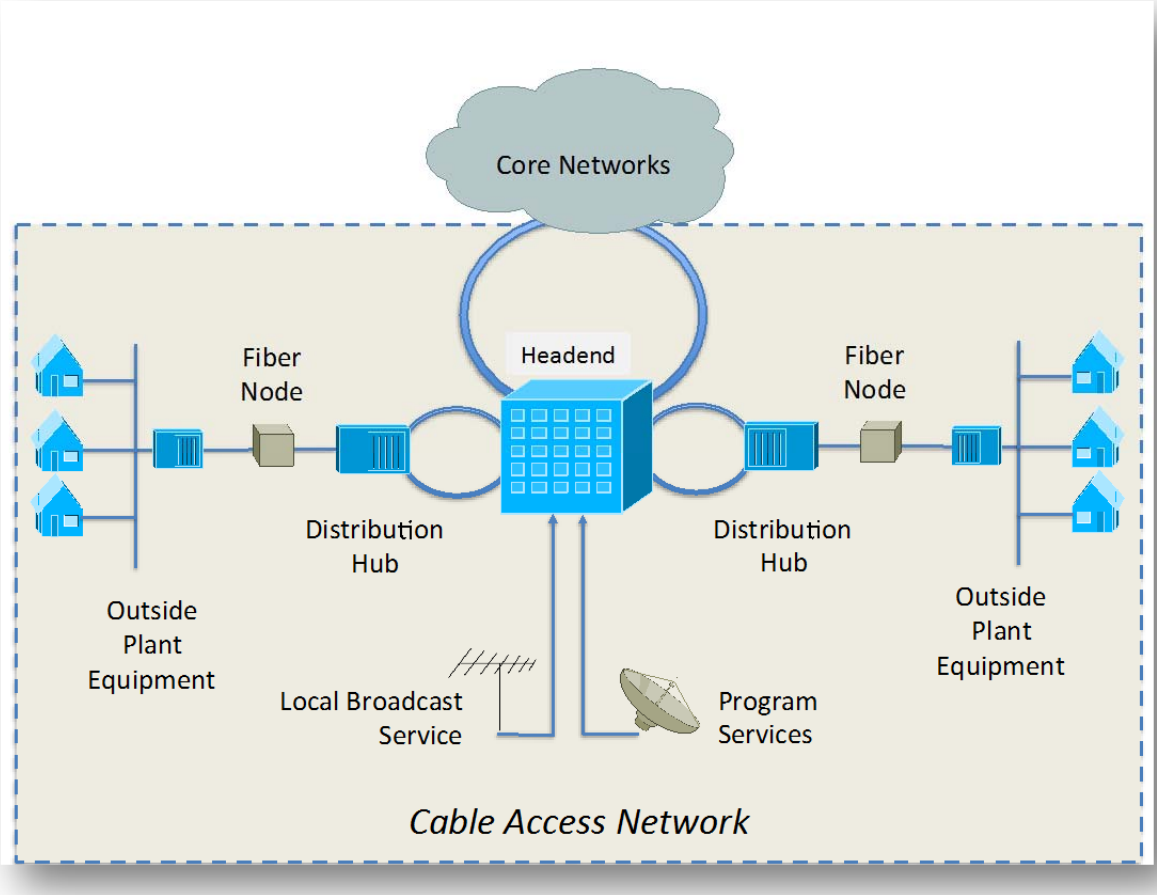


Figure 5 Cable Access Network

The three-level topology is comprised of six major components:

i. **Headend**: The headend serves as the master facility for receiving voice, video, and data signals for processing and distribution over the cable access network. Headends are typically connected to the core network to provide the cable

company's users with connectivity to voice and data communications networks including the Internet.

ii. **Distribution Hub**: The distribution hubs are intermediate process points in the HFC network. The distribution hubs are typically connected to the headend using redundant fiber optic ring architecture. The distribution hubs feed a number of fiber nodes.

iii. **Fiber Node**: The fiber nodes provide the interface between the optical signal, coaxial cable trunk, and distribution cables. The fiber node converts the optical signal into an RF signal for last mile distribution.

iv. **Outside Plant Equipment**: These are small vaults or huts that house cable equipment supporting a specific neighborhood. In addition to housing the supporting equipment, these vaults or huts are where the commercial power is mixed with the RF signals on the coaxial cable to provide power to the opto-electronics in the fiber nodes and the RF amplifiers.

v. **Antenna**: Antennas are used to receive the local over the air channels as well as the cable program networks from the satellites for regeneration and transmission on the cable access network.

vi. **Customer Premise Equipment**: This is the equipment that is placed in the end user's premise to connect to the cable system to receive the services (voice, video, and/or data).

C. Cable Core Network

Cable systems include a core network that links their access network(s) to the communications core infrastructure for voice and data services. Cable systems core network include the operational support systems (OSS) that are used to provision, monitor, and maintain the cable network. Included in the OSS are the billing systems; authentication, authorization and access (AAA) systems, provisioning, monitoring systems, and number lookup systems like domain name servers (DNS).

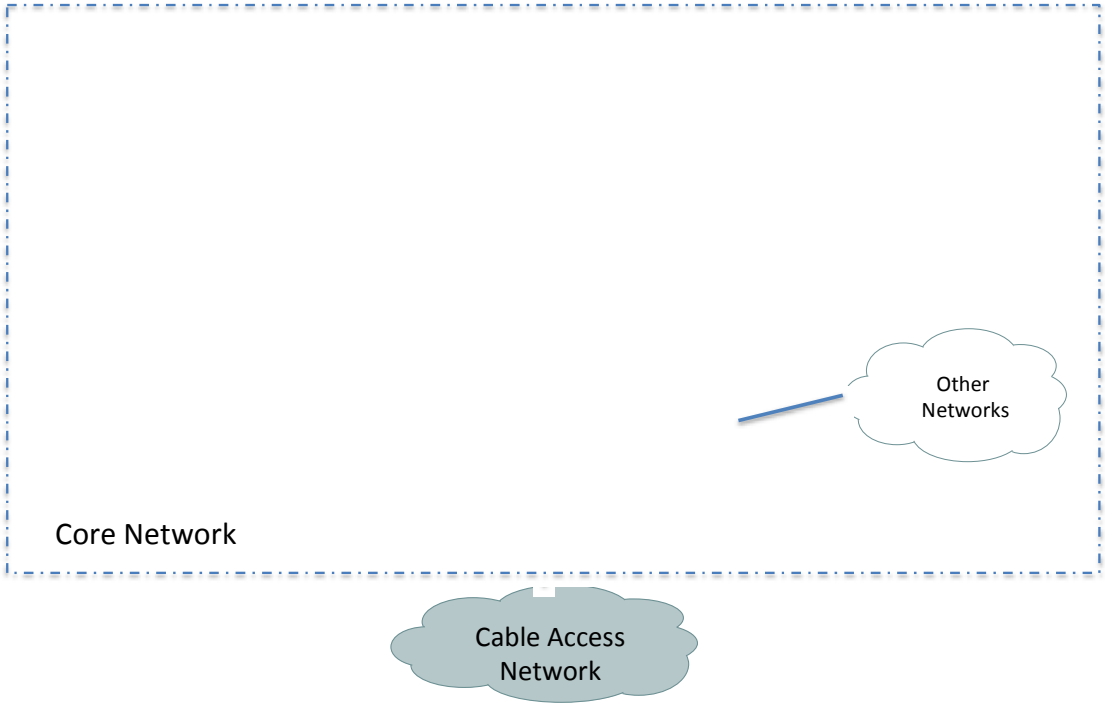


Figure 6 Cable Core Network Infrastructure

Connected to the core network are also the network operations center and customer care centers. The core network is also the gateway to the third party providers, commercial data centers for services such as cloud based services, and access to other networks like the PSTN and Internet.

D. Cable Services

Together the cable access and core network are the "cable network" for delivering voice, video, and data services that includes Internet access.

Voice

Voice service is provided using VoIP technology and is deployed using the same IP-based platform that delivers high-speed Internet access service to cable modems. A number of components are involved in the delivery of the voice service. First is the customer

gateway, sometimes referred to as a multi-media terminal adaptor, that translates call signals to the network call signaling (NCS) protocol used on the cable network for placing voice calls. This gateway may be a standalone unit or it may be embedded into a cable modem. The gateway connects over the HFC network to the cable modem termination system (CMTS) that is located in the headend. The CMTS then interfaces to the voice-switching infrastructure via the core networks routing and switching infrastructure. The voice infrastructure includes the media and signaling gateways for routing the voice traffic to its endpoint that may reside within the access network or off-net in the PSTN.

Video

The video services typically include both local broadcast television affiliates, regional, nationwide programming, and video-on-demand programming. All of these signals are received at the headend and processed to allow it to be put on the network as a channel. These signals are combined together using a process known as frequency division multiplexing for transport to the distribution hubs in the network.

Data

High-Speed Data (HSD) includes Internet access data. HSD uses a cable modem that acts as an Ethernet bridge to convert the data from the customer's home network to a format compatible with the HFC access network. The cable modem interfaces with the CMTS at the headend or distribution hub that in turn connects to the Internet via the core networks switching and routing infrastructure. The CMTS interfaces with other components such as the DNS server, Dynamic Host Configuration Protocol (DHCP) server for the AAA, configuration servers (TFTP) for provisioning, network time protocol (NTP) for time-synchronization, and the subsystems of the operational support system.

E. Areas of Critical Focus or Assets

Based upon the NSRA and the analysis performed by the cable segment group, the cable segment group decided to focus the cable critical infrastructure use case and sample profile on the cable network core infrastructure as outlined in **Figure 6** and described in Section V, which, if disrupted, would have the greatest impact on service availability on a national or regional basis.

It is important to note that the cable segment group is NOT indicating its view that the cable network core should be considered critical infrastructure under the President's recently issued Executive Order, which designates that determination to the Department of Homeland Security.

The cable segment group excluded the access networks and other components of the cable network infrastructure because, while these elements may have some exposure to cyber threats, any incident would largely be locally or regionally focused. Further, while the Domain Name System (DNS) may be in scope, the issues presented by DNS also include

other parties in the ecosystem. Thus, while the cable segment group can provide some DNS practices specific to cable service providers, this topic was viewed to be out of scope for this group. With that said, there was general consensus that the government as a whole should consider addressing the broader ecosystem challenges for DNS and routing security.

VI. Critical Services

The cable segment focused primary on ensuring the reliability and integrity of cable core infrastructure as noted above which is supporting infrastructure for a wide variety of communications services including voice, voice and high-speed data services.

VII. Alignment with the NIST Cybersecurity Framework

The cable segment utilized the NIST cybersecurity framework as a master guideline in order to tailor its applicability to the cable network, organized it in way that can be used by cable operators to examine their network vulnerabilities, and prioritized the approach to risk mitigation for implementation of a strategy.

The cable segment took the NIST framework and applied a 4-element lens in order to create a custom template that is designed to ensure full functioning of our critical infrastructure as the primary objective. Initially, we examined the NIST framework for applicability to protecting cable's critical infrastructure as it has been defined in this document. Each element was considered as whether or not to be in scope to this definition, and subsequently included in a master list if the condition was met. After this initial scoping exercise, the cable segment established a categorization based on 3 tests designed to group each framework element in regard to how each one directly supports the primary objective of maintaining the integrity of our critical communications infrastructure.

VIII. Application Methodology

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
ID.AM-1: Physical devices and systems within the organization are inventoried	In Scope	Asset management includes those devices that make up the service delivery network (voice, IP, data) and their underlining core infrastructure. (not including end user devices)	3	3
ID.AM-2: Software platforms and applications within the organization are inventoried	In Scope		3	3
ID.AM-3: Organizational communication and data flows are mapped	In Scope		3	3
ID.AM-4: External information systems are catalogued	In Scope		3	3
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	In Scope		3	3
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	In Scope		3	3
ID.BE-1: Organization's role in the supply chain is identified and communicated	In Scope	Security reviews/analysis (due diligence) of devices as they are being brought into the infrastructure and communicated to internal management	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	Application	Criticality	Difficulty
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
		and third parties.		
ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated	In Scope	An organizations place in maintaining the core network within the Cable sector is known and communicated within the organization (C Suite) and external agencies and groups. How do we peer with each other, how do we exchange info (voice, data, video). It is known up through the organization, what their role is in critical infrastructure.	3	3
ID.BE-3: Priorities for organizational mission, objectives and actives are established and communicated	In Scope	Prioritizes for an organizational mission, objectives and activities around protecting the core network are established and communicated.	3	3
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	In Scope	Dependencies and critical functions (i.e. electrical, cooling, fuel supplies, etc.) needed for supporting delivery of critical services are identified and understood. (What is critical is defined in the NSRA	3	3
ID.BE-5: Resilience requirements to support delivery of critical services are established	In Scope	Defined in Disaster Recovery Plans, Continuity Plans.	3	3
ID.GV-1: Organizational information security policy is established	In Scope	No further definitions are needed.	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	In Scope		3	3
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	In Scope		3	3
ID.GV-4: Governance and risk management processes address cybersecurity risks	In Scope		3	3
ID.RA-1: Asset vulnerabilities are identified and documented	In Scope	No further definitions are needed.	3	3
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	In Scope		3	3
ID.RA-3: Threats, both internal and external, are identified and documented	In Scope		3	3
ID.RA-4: Potential business impacts and likelihoods are identified	In Scope		3	3
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to	In Scope		3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
determine risk				
ID.RA-6: Risk responses are identified and prioritized	In Scope		3	3
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	In Scope	No further definitions are needed.	3	3
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	In Scope	Expressed through your risk policies. Corporate security policy is your risk tolerance.	3	3
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	In Scope	Covered by our risk assessment in the NSRA.	3	3
PR.AC-1: Identities and credentials are managed for authorized devices and users	In Scope	No further definitions are needed.	3	3
PR.AC-2: Physical access to assets is managed and protected	In Scope	Physical access to the core network assets is managed including any unmanned remote sites.	3	3
PR.AC-3: Remote access is managed	In Scope	Remote accesses to components that make up the core network are managed.	3	3
PR.AC-4: Access permissions are managed, incorporating the principles of least	In Scope	Access permissions are managed, incorporating principles of least privilege and separation of duties on	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
privilege and separation of duties		systems and devices within the core network.		
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	In Scope	Operators will have their management interfaces to the core network segregated from the public internet	3	3
PR.AT-1: All users are informed and trained	In Scope	All identities that support the core network are informed and train.	3	3
PR.AT-2: Privileged users understand roles & responsibilities	In Scope	All identities with privileged accounts understand their roles and responsibilities in securing the core network.	3	3
PR.AT-3: Third-party stakeholders (e.g., suppliers customers, partners) understand roles & responsibilities	In Scope	Third Party Stakeholders are external organizations that do work to support the core network. (Does not include customers)	3	3
PR.AT-4: Senior executives understand roles & responsibilities	In Scope	No further definitions are needed.	3	3
PR.AT-5: Physical and information security personnel understand roles and responsibility	In Scope	No further definitions are needed.	3	3
PR.DS-1: Data-at-rest is protected	In Scope	Limited to the scope of the core network assets.	3	3
PR.DS-2: Data-in-transit is protected	In Scope		3	3
PR.DS-3: Assets are formally managed throughout removal, transfers and disposition	In Scope		3	3
PR.DS-4: Adequate	In Scope	Adequate capacity	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	Application	Criticality	Difficulty
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
capacity to ensure availability is maintained		during crisis events is maintained.		
PR.DS-5: Protections against data leaks are implemented	In Scope	Data leaks as it applies to the core network.	3	3
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	In Scope	MD5 hashes on firmware, code signing, etc. Appropriate tests are done on solutions before they are put into the core network to verify their security.	3	3
PR.DS-7: The development and testing environment(s) are separate from the production environment	In Scope	The testing environment is a separate network, not connected to the operational environment. Could be either at the MSO facility or at a third party vendor. Where applicable. Some tests have to be done in the production network.	3	3
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	In Scope	Baseline configuration of the elements used to provide the three services is created/maintained.	3	3
PR.IP-2: A System Development Life Cycle to manage systems is implemented	In Scope	No further definitions are needed.	3	3
PR.IP-3: Configuration change control processes are in place	In Scope	A configuration control process is used for all updates and patches to systems within the cable framework scope.	3	3
PR.IP-4: Backups of	In Scope	Backups of systems	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
information are conducted, maintained and tested periodically		within the core network are maintained and tested periodically.		
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	In Scope	Physical operating environment for the core infrastructure.	3	3
PR.IP-6: Data is destroyed according to policy	In Scope	We destroy IP data mappings as defined by policy.	NA	NA
PR.IP-7: Protection processes are continuously improved	In Scope	Protection processes of the core network are continuously evaluated.	3	3
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	In Scope	Sharing with appropriate internal parties (management, board).	3	3
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	In Scope	Response plans and recovery plans for components within the scope of the core network are in place and managed.	3	3
PR.IP-10: Response and recovery plans are tested	In Scope	Response plans and recovery plans for components within the scope of the core network are tested.	3	3
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	In Scope	No further definitions are needed.	3	3
PR.IP-12: A	In Scope	Vulnerability	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	Application	Criticality	Difficulty
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
vulnerability management plan is developed and implemented		management of the assets within the defined core network are developed and managed.		
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	In Scope	Maintenance and repair of core network components as defined in the scope is performed and logged in a timely manner, with approved and controlled tools.	3	3
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	In Scope	Remote maintenance of core network components as defined in the scope is performed in manner that prevents unauthorized access. Most of our networks are remote.	3	3
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	In Scope	Audit/logs of core network components as defined in the scope are determined, documented, implemented, and reviewed in accordance with policy.	3	3
PR.PT-2: Removable media is protected and its use restricted according to policy	In Scope	Removable media is protected and its use on devices within the core network is restricted according to policy.	3	3
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	In Scope	Access permissions are managed, incorporating principles of least privilege and separation of duties on systems and devices within the core network scope.	3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
		(Duplicate of AC-4)		
PR.PT-4: Communications and control networks are protected	In Scope	Out-of-band network controls and communications are protected.	3	3
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	In Scope	A baseline of operational events and data flows for users and systems are established and managed.	3	3
DE.AE-2: Detected events are analyzed to understand attack targets and methods	In Scope	Detected events targeting core network assets are analyzed.	3	3
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	In Scope	Data from events targeting core network assets is used to determine impacts and establish incident thresholds.	3	3
DE.AE-4: Impact of events is determined	In Scope		3	3
DE.AE-5: Incident alert thresholds are established	In Scope		3	3
DE.CM-1: The network is monitored to detect potential cybersecurity events	In Scope	Privileged access to core network assets is monitored to detect potential cybersecurity events.	3	3
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	In Scope	Physical access to core network assets is monitored to detect potential cybersecurity events.	3	3
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	In Scope	Personnel activity involving core network assets is monitored to detect potential cybersecurity events.	3	3
DE.CM-4: Malicious code is detected	In Scope	Anti-virus on servers, scanning mobile	NA	NA

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
		applications before publishing and check if customers have viruses (relates back to PR-DR-6)		
DE.CM-5: Unauthorized mobile code is detected	In Scope	Network is monitored to detect potential cyber security events from self-developed mobile applicants, on the go software applications running on mobile devices.	NA	NA
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	In Scope	Contractors, Cloud service providers, and other authorized parties who can access the network are monitored.	NA	NA
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	In Scope	Core network assets are monitored for unauthorized personnel, connections, devices, and software.	3	3
DE.CM-8: Vulnerability scans are performed	In Scope	Scanning of devices that provide the services of the core network.	NA	NA
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	In Scope	Core network assets are secured with established and reliable detection processes.	3	3
DE.DP-2: Detection activities comply with applicable requirements	In Scope		3	3
DE.DP-3: Detection processes are tested	In Scope		3	3
DE.DP-4: Event detection information is communicated to appropriate parties	In Scope		3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
DE.DP-6: Detection processes are continuously improved	In Scope		3	3
RS.RP-1: Response plan is executed during or after an event	In Scope	The continuous operation of core network assets is ensured through effective preparation and use of incident response plans.	3	3
RS.CO-1: Personnel know their roles and order of operations when a response is needed	In Scope		3	3
RS.CO-2: Events are reported consistent with established criteria	In Scope		3	3
RS.CO-3: Information is shared consistent with response plans	In Scope		3	3
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	In Scope		3	3
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	In Scope		3	3
RS.AN-1: Notifications from detection systems are investigated	In Scope		3	3
RS.AN-2: The impact of the incident is understood	In Scope		3	3
RS.AN-3: Forensics are performed	In Scope		3	3
RS.AN-4: Incidents are categorized consistent with plans	In Scope		3	3

	Scoping		Prioritization	
	In Scope/Out of Scope	**Application**	**Criticality**	**Difficulty**
Sub-Category			1 to 5;1=Not Critical, 5=Most Critical	1 to 5; 1 Most difficult, 5 least difficult
RS.MN-1: Incidents are contained	In Scope		3	3
RS.MN-2: Incidents are mitigated	In Scope		3	3
RS.MN-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	In Scope		3	3
RS.IM-1: Response plans incorporate lessons learned	In Scope		3	3
RS.IM-2: Response strategies are updated	In Scope		3	3
RC.RP-1: Recovery plan is executed during or after an event	In Scope	Assets within the core network will be included in the Recovery Plans and Recovery efforts to include any public relations and communication activities.	3	3
RC.RP-1: Recovery plans incorporate lessons learned	In Scope		3	3
RC.RP-2: Recovery strategies are updated	In Scope		3	3
RC.CO-1: Public related are managed	In Scope		3	3
RC.CO-2: Reputation after an event is repaired	In Scope		3	3
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	In Scope		3	3

IX. Priority Practices

The cable segment's initial scoping review concluded that all of the NIST cybersecurity framework subcategories were in scope as it applies to the cable industry; so all framework elements were utilized in our analysis. After categorization into one of the 3 levels outlined above, the cable segment grouped the elements into a spreadsheet that reflects the analysis.

The categorization of framework elements is as follows:

- Level 1 - Items that without which, critical communication functions are compromised.
- Level 2 - Items that directly support operation of Level 1 elements
- Level 3 – Items that inform and provide services to Level 1 elements

The 24 practices in the table below illustrate a sub-set of the 96 practices from the framework that an enterprise may determine using the methodology described in this report for itself that will have largest benefit.

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

Level 1	Level 2	Level 3
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

X. Use Case – Generic Cable Critical Infrastructure

As defined in Executive Order 13636, Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The definition is taken from section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c (e)).

As noted above in Section V, based upon the NSRA and the analysis performed by the cable segment group, the cable segment group focused on core network as illustrated in **Figure 6**, which, if disrupted, would have the greatest impact on service availability on a national or regional basis.

As noted in the Threat's Segment Report, the threat landscape will continue to evolve. As a result, the profile should support agile and adaptive methods of obtaining threat intelligence and responding to them.

The cable segment group as part of its analysis reviewed the Ecosystem's Segment Report. As noted in this report, the cable segment concurs that the global Internet Ecosystem is not confined to delivery or access "networks", and cable network operators as part of their risk management programs need to take into consideration the broader ecosystem.

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.
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Roles and responsibilities are aligned in effect.
PR.AC-1: Identities and credentials are managed for authorized devices and users	Identities and credentials are established and operational as they relate to access to devices by users.
DE.CM-1: The network is monitored to detect potential cybersecurity events	Monitoring is operational and utilized.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Physical security established and monitored per guidelines in PR.AC-2
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	Monitoring of personnel is active per multiple framework subcategories (PR.AC-1-2-3-4/PR.MA-2/PR.PT-3)
DE.CM-4: Malicious code is detected	Malicious code is found and mediated per DE.CM-1.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	No unauthorized access occurs.
PR.AC-2: Physical access to assets is managed and protected	Physical access controls are in place and effective per established guidelines.
PR.AC-3: Remote access is managed	Remote access controls are active only for those with operational need.
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Access permissions are in place and applied on a need to know and compartmentalized basis.
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	Network is properly designed and operational per security best practices.
PR.DS-2: Data-in-transit is protected	Data transit protection policies and procedures are in place.
PR.DS-4: Adequate capacity to ensure availability is maintained	Capacity planning and management in effect.
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	Remote maintenance is performed per guidelines in PR.AC-3
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Access to systems and assets is performed per guidelines in PR.AC-4

PR.PT-4: Communications and control networks are protected	Protection is established and operational.
RS.RP-1: Response plan is executed during or after an event	Response plan is effective in mitigating further threat.
RS.MN-1: Incidents are contained	Incidents no longer a threat.
RS.MN-2: Incidents are mitigated	Incidents no longer active.
RC.RP-1: Recovery plan is executed during or after an event	Network is back to fully operational status.

XI. Recommendations: Cable Segment

- No new regulations are warranted to address conformity to the NIST Framework as it relates to the cable segment.

- Continued flexibility is essential in the use and conformity to the NIST Framework given the diversity within the cable segment. As noted in the Threats sub-group report, the threat landscape is constantly evolving and requires agile and adaptive methods for managing the risk. Cable network operators are best positioned to understand their cybersecurity risks and should be afforded flexibility to apply the framework to their business needs. The FCC should avoid taking a checklist approach to cybersecurity.

- DHS should continue as the Sector Specific Agency for Telecom in order to advance the established programs and evolution of the NIST Framework. The FCC should continue to partner with industry via the Government Coordinating Council (GCC) and/or via voluntary measures such as CSRIC.

9.3 SATELLITE SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

I. Executive Summary

The Satellite Segment is a subgroup within the CSRIC Working Group 4 effort focused on adapting the NIST Cybersecurity Framework, and its emphasis on cybersecurity risk management, to the satellite communications industry. Consistent with the emphasis of the NIST Cybersecurity Framework, the focus of the Satellite Segment's analysis was on critical infrastructure components of the satellite industry and critical satellite services. With this scope in mind, the satellite segment examined the risk management categories and subcategories of the NIST Framework, identified those most relevant to the protection of critical infrastructure and critical service, and evaluated them further based on their effectiveness and difficulty. The satellite segment then applied this modified framework to a hypothetical example of a cybersecurity vulnerability affecting the satellite industry to illustrate how satellite service providers already apply these concepts in their risk management practices, and to suggest mechanisms for more fully integrating the risk management principles of the NIST Cybersecurity Framework.

The analytical framework set out below represents a consensus prioritization of the NIST Framework's subcategories, agreed to by a diverse group of satellite industry experts, and can be used as a model by satellite industry members seeking to implement the NIST Framework in their organization. The satellite segment subgroup developed this prioritized adaptation of the NIST Cybersecurity Framework based on rigorous analysis and developed a use case illustrating how the framework can be applied practically within an organization, however, this report is not intended to provide a checklist or prescriptive solution for cybersecurity risk management. Perhaps more important than the end product, in terms of managing cybersecurity risk, is the analytical process of identifying the scope of infrastructure components to be protected; examining the NIST Framework's recommendations in light of an organization's own priorities, capabilities, and vulnerabilities; and developing an implementation that is robust, self-reinforcing, and catered to the specific needs of an organization.

II. Introduction

The Satellite Segment is a subgroup within the CSRIC Working Group 4 effort focused on adapting the NIST Cybersecurity Framework, and its emphasis on cybersecurity risk management, to the satellite communications industry. As illustrated below, the satellite segment subgroup had participation from a wide cross-section of the satellite industry, including service providers in the fixed, mobile, and direct-to-home/broadcasting satellite services, both government and consumer-focused service providers, and manufacturers of satellite communications devices and infrastructure.

Satellite communications services are key to many critical infrastructure sectors. Four of the critical infrastructure sectors most reliant on satellite services are Emergency Services, Defense Industrial Base, Information Technology, and Communications. In each of these sectors, satellite communications provide a primary mechanism for mission critical communications. However, satellite communications are unique among communications technology in terms of their ubiquity and survivability, and therefore have additional importance and backup systems for many other sectors. Additional components of critical infrastructure that might subscribe to

satellite services for remote operations or emergency backup include Agriculture and Food; Water; Dams; Healthcare and Public Health; Government Facilities; Commercial Facilities; National Monuments and Icons; Energy; Nuclear Reactors, Materials, and Waste; Transportation Systems; Banking and Finance; Chemical; Critical Manufacturing; and Postal and Shipping.

The satellite industry has a long history and substantial experience in analyzing and improving security, even beyond that of some other commercial communications technologies. In particular, to support the demands of military and government users, many satellite operators already comply with various controls, checklists, and certifications – including DoD Information Assurance requirements, international standards, and other criteria. Because of the nature of satellite communications technology, many military and government services share infrastructure components and systems with commercial and enterprise services – both in the space-based and ground-based segments of the system. This means that satellite communications service providers are leaders in areas like encryption, access control, and overall system hardness. These protections make the entirety of satellite systems – including non-Federal users – safer.

Satellite Segment Subgroup Members

Name	Company
Donna Bethea Murphy - Chair	Iridium Communications Inc.
Anthony Acosta	Northrop Grumman
Andre Christian	O3b Government
Shelton Darensburg	ViaSat
Steve Doiron	Echostar/Hughes Network Systems
Vinit Duggal	Intelsat
Andrew D'Uva	Providence-Access
Victor Einfeldt	Iridium Communications Inc.
Rick Foster	Lockheed Martin
Aniruddha Karmarkar	Lockheed Martin
Greg Kulon	Boeing
Ethan Lucarelli	Wiley Rein LLP
Jennifer Manner	Echostar
Martin Pitson	Telesat
Joel Rademacher	Iridium Communications Inc.
Alan Rinker	Boeing
Derek Schatz	Boeing
J.J. Shaw	O3b Government
Fred Travis	Iridium Communications Inc.

III. Objective, Scope and Methodology

A. Objectives

The mission statement of CSRIC IV Working Group 4 is to develop voluntary mechanisms to provide macro-level assurance to the FCC and the public that

communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise through the application of the NIST Cybersecurity Framework, or an equivalent construct. These 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).

To fulfill this mission, the satellite subgroup analyzed the NIST Cybersecurity Framework version 1.0 from the perspective of the satellite industry to conform the practices and processes described therein for the satellite segment of the communications sector. The NIST Cybersecurity framework is intended to be applied flexibly according to the needs and characteristics of a particular enterprise or industry. At its core, the Framework is a voluntary mechanism that can be adapted and incorporated into an organization's practices. To facilitate that process, the satellite segment Subgroup examined the categories and subcategories of practices described in the NIST Framework to identify those most relevant to protecting critical infrastructure and critical services. Combined with input from the various Working Group 4 Feeder Groups, the satellite segment Subgroup composed an example target profile for protection of critical satellite services, and developed an illustrative use case of how the Framework might be implemented by a satellite communications service provider.

B. Scope

Given the initial focus of the NIST cybersecurity framework in critical infrastructure, the satellite segment group focused initially on identifying the aspects of the satellite communications system that should be considered critical infrastructure and the critical services provided by satellite communications. These critical infrastructure and critical services define the scope of the NIST Framework alignment discussed below in Section IV.

Working Group 4 determined that the definition of critical infrastructure should be consistent with the definition outlined in President Obama's Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity," which states that critical infrastructure includes those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[43]

Further, in 2012 the Communications Sector, in partnership with Department of Homeland Security (DHS), completed the 2012 Risk Assessment for Communications (referred to going forward as the National Sector Risk Assessment or NSRA), which assessed physical and cyber threats to the communications infrastructure. The risk

[43] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013) [hereinafter *EO 13636*].

assessment was intended to further the goals of the Communications Sector Specific Plan developed jointly with DHS in 2010, to identify and protect national critical network components, ensure overall network reliability, maintain "always-on" service for critical customers and quickly restore critical communications functions and services following a disruption. The satellite segment subgroup agreed with the other Segment groups that the scope of its efforts should build upon the work already completed in the NSRA.

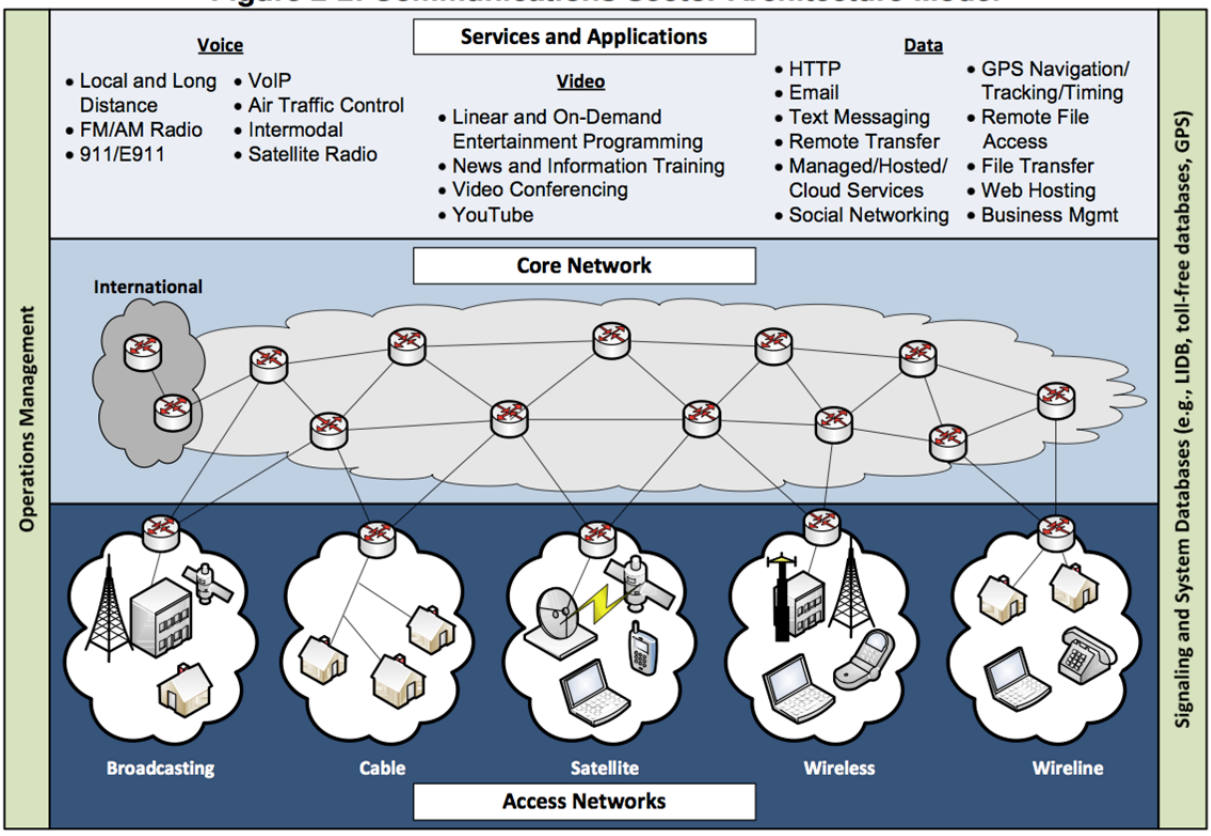
Taking the NSRA model as a starting place, the satellite subgroup then developed its own models of satellite systems architecture from which it extracted and identified the critical infrastructure elements. These critical elements delineate the scope of assets intended to be protected through the further analysis below. The group also identified the critical services provided by satellite communications systems. Ensuring availability of these services is a goal of the cybersecurity risk management processes described in the Analysis section of this report.

A key assumption of the scoping exercise is that government owned or controlled satellite systems are outside of the scope of the working group's analysis, as the subgroup is an industry segment group, and private sector entities may not have primary or exclusive control over cybersecurity risk management for those Federal systems. Importantly, however, many government/military services also operate over commercial satellite systems, and these services have increased cybersecurity needs often requiring commercial systems to meet Federal security specifications. This leveraging of commercial infrastructure has the additional benefit of increasing the overall security of assets used in the provision of commercial services.

NSRA Architectural Model & Assumptions

The Communications National Sector Risk Assessment (NSRA) architecture model[44] (see Figure below) identifies national level communications architecture elements that are at elevated risk and serves as a baseline to prioritize the communications infrastructure.

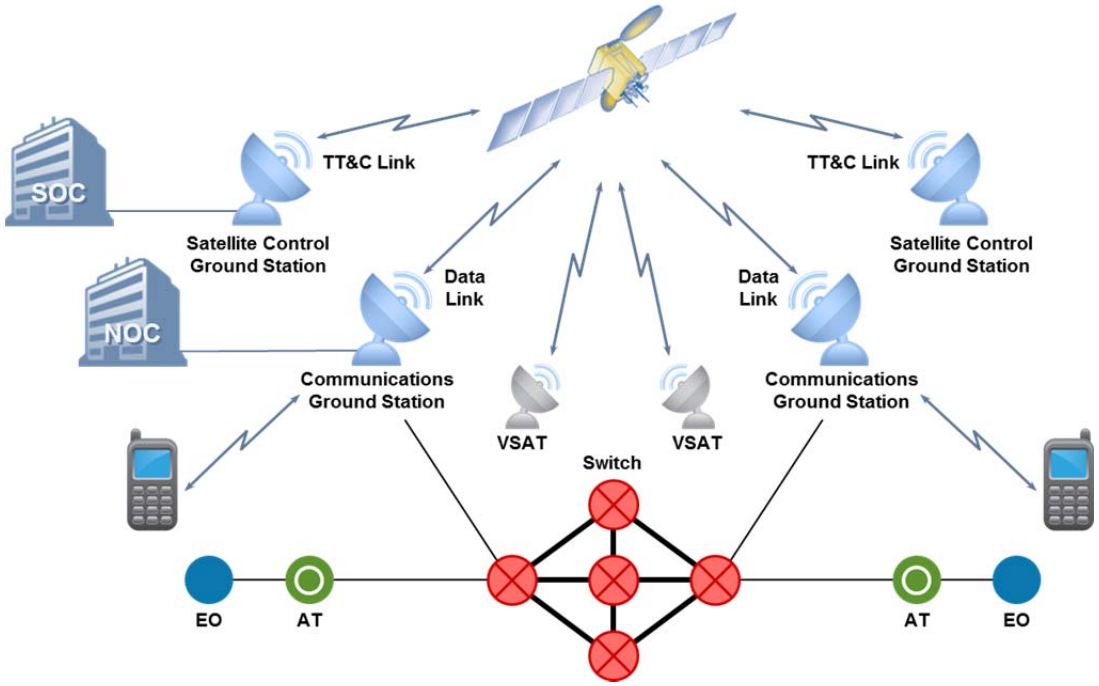
Figure 2-2: Communications Sector Architecture Model



The NSRA provides a high level reference model for all segments of the Communications Sector including broadcast, cable, satellite, wireless and wireline. Building upon the NSRA Model, the satellite segment developed the two segment-specific models below, which represent example Fixed Satellite Service (FSS) and Mobile Satellite Service (MSS) system architectures.

[44] *See* Department of Homeland Security, *Critical Infrastructure Partnership Advisory Council Annual Update* (2012), *available at* http://www.dhs.gov/sites/default/files/publications/cipac-%202012-final-508-%20compliant-%20version.pdf.

Fixed Satellite Service (FSS)



Mobile Satellite Service (MSS)

Based on the CSRIC WG 4 Satellite Segment Model and the definition of critical infrastructure contained in Executive Order 13636[45] the following elements and services are considered for purposes of the scope of this Segment report.

1) Identify Areas of Critical Focus or Assets

Satellite communications system architectures are each unique and purpose-built to best serve the needs of the network operator's target market. While there is less uniformity among satellite systems than might exist in other segments, there are some core elements and functions similar across most systems.

Satellite/Space Vehicle: The space-based component of the communications platform. Satellite systems can come in a variety of configurations (GSO, NGSO) and orbits (LEO, MEO, GEO). Service in a geographic region may be provided by a single spacecraft (e.g., in a GSO FSS system) or through multiple vehicle constellation (e.g., in a NGSO MSS system). The satellite has the following critical components:

1. Payload (receiver, amplifier, high gain antenna)
2. Bus (propulsion, attitude, thermal, command processor)

Telemetry, Tracking, and Command (TT&C) Facilities/Spacecraft Operations Center (SOC): Functionality to maintain health and safety of the spacecraft. It is assumed that SOC redundancy is available to maintain operations with switching timelines that support control transition should one site become unavailable/unusable. The SOC may have the following critical components:

1. Large parabolic antenna
2. RF equipment
3. Command processor
4. Ranging system
5. Inter-facility link
6. Control center
7. Flight dynamic control system
8. Radio Frequency Auto Tracking (RFAT)
9. Generator/UPS

Network Control Center/Network Operations Center (NOC): Depending on service type, the operator may require ability to add new users onto active links (*e.g.*, bring up communications services to mobile emergency responders if not previously initiated). NOC operations not likely to be critical include billing/customer care, database/archiving, change control, planning, network management for non-critical users. Critical areas needed to be maintained will be dependent on NOC architecture and type of emergency service required.

1. Account activation system
2. Network management system
3. Carrier monitoring

[45] *See EO 13636*.

4. Generator/UPS
5. Monitoring center
6. Terrestrial link to gateways

Gateway facilities: Ground equipment and facilities for managing subscribers, controlling subscriber access to services, providing billing for services, and providing interoperation between subscriber sessions and other networks. Depending on the system architecture, gateway components may include:

1. Large parabolic antenna
2. RF equipment
3. Baseband equipment
4. Fiber optic backbone
5. M&C sub-system
6. Generator/UPS
7. Mobile Switching Center
8. Access Network Controller (ANC)
9. Location Server
10. Servers for Various Services
11. Subscriber Database

Teleport Network (TPN): Terrestrial mesh of multi-terminal ground stations (Teleports) providing bulk space-ground connectivity, as well as interconnecting the various elements of Operations and Gateway Segments; each Teleport (TP) is managed by a Teleport Controller (TPC) and includes a number of Feeder Link Terminals (FLTs).

1. Teleport Controller (TPC)
2. Antenna
3. RF equipment
4. Baseband equipment
5. Fiber optic backbone
6. Monitor and Control (M&C) sub-system
7. Generator/UPS

Uplink Facility: This facility provides uplink of content to be distributed to subscriber equipment.

1. Antenna
2. RF equipment
3. Baseband equipment
4. Fiber optic backbone
5. M&C sub-system
6. Generator/UPS

Radio Frequency Links: The RF links themselves are a core component potentially subject to attack. These provide communications to the satellite (which can include service links, feeders, or TT&C) and downlink communications to subscriber equipment.

1. Uplinks

2. Downlinks
3. Intersatellite Links
4. Feeder links
5. Primary and backup command and control

2) Identify Critical Services

There are four of the Critical Infrastructure sectors that are more dependent on use of satellite services, including;

- Emergency Services
- Defense Industrial Base
- Information Technology
- Communications

Additional Critical Infrastructure items could also be subscribing to satellite services for remote operations or as emergency backup. These include: Agriculture and Food; Water; Dams; Healthcare and Public Health; Government Facilities; Commercial Facilities; National Monuments and Icons; Energy; Nuclear Reactors, Materials, and Waste; Transportation Systems; Banking and Finance; Chemical; Critical Manufacturing; and Postal and Shipping.

The Federal Communications Commission and International Telecommunication Union define three categories of satellite communications services, each of which support distinct critical services.

Fixed Satellite Services (FSS): A satellite service where the earth stations do not move during transmission. FSS supports voice, video, and data, which can be used for broadcast distribution, point-to-point, and point-to-multipoint communications.

- Terrestrial Infrastructure Emergency Backup: Expected to be primarily mobile users, civil emergency response.
- Satellite electronic news gathering
- Emergency Response Communications
- Connectivity to Rural Communities – Certain remote communities are exclusively dependent on satellite for external communications (PSTN/data)
- Supervisory Control and Data Acquisition (SCADA) – Used to gather data and control facilities such as pipeline, power generation and distribution, remote air traffic control facilities, rail facilities.
- Access to funds – ATM and point of sale so local population can access funds in areas where terrestrial infrastructure is inoperative.

Mobile Satellite Services (MSS): A satellite service designed to support mobile ground stations. MSS supports voice, data, and broadcast services.

- Telephony: Circuit Switched voice and data calls that communicate real-time or near real-time information.

- Messaging: Short messages that can either be person-to-person, machine-to-machine, or many-to-many as the case with burst messaging. Critical for status updates and when voice calls aren't possible to make. Messages can also be queued for delivery if service is interrupted temporarily.
- Military/Tactical Communications: Systems that support Military Communications are likely to have more importance with regards to overall security, health and safety of the population and the warfighter, and require additional protections. Such protections would likely include secure/protected satellite TT&C and mission communications (*e.g.*, NSA Certified cryptography, Information Assurance, and possibly anti-jam protection from both nuisance interference and intentional attack). Further protections for communications supporting active operations may include physical security of all satellite and network operations areas and teleport/gateway hardware to include restricted access and stay-out zones (*i.e.*, physical distance in kilometers from public access area to hardware installations to prevent physical or electronic attack). Additional separation (electronic guards and or physical separation) may be required for separation from public interfaces to minimize the potential for cyber-attack.
- Mobile data (high speed/short burst)
- Machine-to-Machine
- GMDSS: Internationally agreed-upon set of safety procedures, types of equipment, and communication protocols used to increase safety and make it easier to rescue distressed ships, boats and aircraft. The system is intended to perform the following functions: alerting (including position determination of the unit in distress), search and rescue coordination, locating (homing), maritime safety information broadcasts, general communications, and bridge-to-bridge communications.
- Emergency Response communications: Emergency Services to remote areas with no terrestrial infrastructure (e.g. support to firefighters in remote areas of Western US).

Broadcasting-Satellite Service (BSS)/Direct-to-Home (DTH): A receive-only service where information flows from a central hub station to a large population. Typical uses are subscription-based television or radio services.

- Emergency Alert Broadcasts
- Local news and weather information

C. Methodology

The work of the satellite segment Subgroup was conducted in 4 main phases. First, the Subgroup defined the scope of the analysis, which, drawing from Executive Order 13636 and discussions with the other Segment and Feeder Groups, was determined to be limited to critical infrastructure and services. Next, the Subgroup applied an analytical framework developed in conjunction with the larger Working Group 4 to consider whether each

functional area, category and sub-category of the NIST framework was in or out of scope, how they may be applied, their effectiveness in protecting against cyber threats, and difficulty to implementation. In conducting this analysis the Subgroup also collaborated with and considered input related to barriers to implementation and the various threats identified by the Threats Feeder Group. Third, the Subgroup developed an illustrative use case to demonstrate how an enterprise might implement the risk management approach of the NIST Framework in its own practices. Finally, the sub-working group shared findings and recommendations and exchanged views with the other sub-working groups and collaborated in the production of the overall WG 4 report.

The work of the subgroup largely was conducted telephonically through regular conference calls within the satellite segment, in conjunction with other feeder and segment groups, and as a working group as a whole. The satellite segment Subgroup also participated in several face to face meetings with the entirety of WG4 and exchanged numerous drafts and input documents over email.

IV. Results and Findings

A. Alignment with NIST Cybersecurity Framework

To align with the NIST Cybersecurity Framework, this document will assist participants in the satellite segment by tailoring the framework's categories and subcategories to best serve the segment's unique cybersecurity challenges. In doing so, the satellite segment evaluated each category and subcategory in terms of its criticality, difficulty, and effectiveness.

Criticality:

The satellite segment group approaches the entire project from the perspective of protecting critical services and critical infrastructure. When it examined the categories and subcategories of the NIST framework to determine which were most applicable to the satellite segment, the satellite segment group eliminated those that were not related to protecting critical services and critical infrastructure as out of scope for this analysis.

Difficulty:

Difficulty was determined as a product of cost for implementation (in terms of money as well as other resources), complexity, time taken to complete the process, human factors, and likelihood of completing the task.

Effectiveness:

Effectiveness was construed as a measurement of how directly the process impacts the likelihood or severity of a subsequent cybersecurity event. Processes that produce an identifiable result in terms of reduced vulnerability were deemed more effective. In evaluating effectiveness, the satellite segment subgroup assumed that the process was successfully completed (as likelihood of completion is accounted for in difficulty) and looked at the result of the process.

Further assumptions:

- All satellite service providers were seen as "medium" businesses. The resources required to develop and launch a satellite system generally preclude "small" operators, and to the extent there are small entities, they are not involved in the provision of critical services. When viewed in the context of the overall communications sector, satellite operators are much smaller than large telcos, and thus are not "large" entities.
- Internal policies/procedures and government regulations are assumed to be followed and implemented faithfully. There is no need for a separate process instructing the enterprise to follow these policies.
- All processes and practices contemplated by the subcategories were considered as limited in applicability to critical services and infrastructure. Thus an inventory of devices and systems was assumed to refer to devices and systems used in critical services and infrastructure.
- Continuous process improvement and self-reflection is assumed.

The matrix below collects the satellite segment's analysis of the NIST Framework's subcategories according to the criteria discussed above. Subcategories that were determined not related to protecting critical infrastructure and services were not included on the matrix. The remaining subcategories were assigned a value for difficulty and effectiveness, through application of the definitions set forth above. For purposes of prioritization, a higher numerical value in Difficulty corresponded to a lower actual level of difficulty, whereas a higher value in Effectiveness suggested a greater and more identifiable impact when the subcategory is successfully implemented. Where the group felt that additional explanation of the application of the subcategory was warranted, this was included in the Application column.

While the numerical values are assigned in a way that could accommodate prioritization of the subcategories through looking at the highest aggregate score, the analytical matrix below is not intended for uniform application and simple prioritization. In some cases, difficult to implement subcategories might have a lower aggregate score than their actual importance should suggest. Moreover – and in keeping with the flexibility inherent in the NIST Cybersecurity Framework – this analytical matrix is intended to be illustrative and to provide a model for companies to follow in adapting the NIST Framework to their own operations. An application of the NIST Framework done in the context of the specific needs and capabilities of a particular company will be a much more effective tool for cybersecurity risk management.

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
Identify (ID)	Asset management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	Organizations need to assess what is mission critical and what is administrative. Extremely effective, it is essential to know what you have.	4	5
		ID.AM-2: Software platforms and applications within the organization are inventoried	Difficulty might increase with scale of organization	4	5
		ID.AM-3: Organizational communication and data flows are mapped	It is essential to map and understand the flows within critical mission threads, and to understand dependencies that create risks of interruption of communications/ processes.	3	3
		ID.AM-4: External information systems are catalogued		4	5
		ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	Resources should be prioritized based on mission criticality; business and corporate functions are not critical to sustaining the mission. Difficult to make distinctions between absolute mission critical, etc. There are not a lot of tools that can do that automatically.	2	3

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
	Business Environment (ID.BE)	ID.BE-1: Organization's role in the supply chain is identified and communicated		3	2
		ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated		3	2
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established		2	2
		ID.BE-5: Resilience requirements to support delivery of critical services are established		3	4
	Governance (ID.GV)	ID.GV-1: Organizational information security policy is established		4	3
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Related to establishing and governing specific people to implement security policy	3	3
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed		1	3
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented		2	5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	Difficulty is acquiring and identifying good information for critical infrastructure.	2	3

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 and protected		5	4
		PR.AC-3:Remote access is managed		2	4
		PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties	Important for the industry to move in this direction.	2	4
		PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate		3	4

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
		PR.AT-2: Privileged users understand roles & responsibilities	Implementing effective training across levels of an enterprise is difficult.	2	3
		PR.AT-4: Senior executives understand roles & responsibilities		2	3
		PR.AT-5: Physical and information security personnel understand roles and responsibility		4	5
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected		4	5
		PR.DS-2: Data-in-transit is protected		4	5
		PR.DS-3: Assets are formally managed throughout removal, transfers and disposition		2	4
		PR.DS-4: Adequate capacity to ensure availability is maintained		3	4
		PR.DS-5: Protections against data leaks are implemented	Publicly available systems can be leveraged to accomplish this	3	4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity		2	4
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained		4	4
		PR.IP-3: Configuration change control processes are in place		4	4

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
		PR.IP-4: Backups of information are conducted, maintained and tested periodically		3	4
		PR.IP-7: Protection processes are continuously improved	Continuous improvement of processes should be a global activity.	4	3
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	Information about patches, improvements, and upgrades on protection technologies needs to be disseminated throughout the community.	2	3
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed		1	2
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	The level of detail included in HR practices would depend on the policy and needs of the enterprise; however these processes need to address risks of malicious insider attacks.	3	2
		PR.IP-12: A vulnerability management plan is developed and implemented	[covers ID-RM, and RS.RM-3]	3	2
	Maintenance (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools		4	4

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
		PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access		3	2
Detect (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed		3	3
		DE.AE-2: Detected events are analyzed to understand attack targets and methods		4	4
		DE.AE-4: Impact of events is determined	Should be done at the appropriate level and limited to critical functional capabilities. To detect an event and develop an appropriate response it is important immediately to know the impact to critical network components.	4	4
		DE.AE-5: Incident alert thresholds are established		4	4
	Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events		4	3
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events		4	3

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	Limited to addressing the malicious insider threat. Ideally this monitoring is tied to a threshold or trigger—not actively monitoring all employee activity. Goal is to identify unauthorized access/high-risk activity.	2	4
		DE.CM-4: Malicious code is detected		3	4
		DE.CM-5: Unauthorized mobile code is detected	Can be system-wide/firmware, or code in an individual device. Both are critical.	1	5
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Outside firms/contractors can be a source of breaches. Need to monitor what they are doing.	1	5
	Detection Processes (DE.DP)	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability		4	4
		DE.DP-6: Detection processes are continuously improved	An overall statement of continuous process improvement should be made.	4	3
Respond	Communications (RS.CO)	RS.CO-2: Events are reported consistent with established criteria		3	3
		RS.CO-3: Information is shared consistent with response plans		3	3

Function	Category	Subcategory	Application	Difficulty (lower is more difficult)	Effectiveness (higher is more effective)
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans		3	3
	Analysis (RS.AN)	RS.AN-1: Notifications from detection systems are investigated		3	3
		RS.AN-2: The impact of the incident is understood		2	2
	Mitigation (RS.MI)	RS.MI-1: Incidents are contained		2	3
		RS.MI-2: Incidents are mitigated		2	4
	Improvements (RS.IM)	RS.IM-1: Response plans incorporate lessons learned		4	2

B. Findings

- Satellite system operators already have complex and rigorous security and risk management processes in place, and the NIST Framework provides an effective, flexible mechanism for analyzing, improving, and communicating internally about those established practices.
- In particular, to support the demands of military and government users, many satellite operators already comply with various controls, checklists, and certifications – including DoD Information Assurance requirements, international standards, and other criteria applicable to the entire system. This means that satellite communications service providers are leaders in areas like encryption, access control, and overall system hardness. These protections make the entirety of satellite systems – including non-Federal users – safer.
- Although there are some common architectural principles, as discussed in the Scope section of this report, each satellite system is technologically unique to an extent not present in any other segment of the Communications sector.
- The NIST Framework is effective because it identifies functional categories of processes that industry members can self-tailor according to their particular needs and capabilities. Rigid, prescriptive approaches will not best serve the goals of increasing security and better managing risk.
- The analytical framework above represents a consensus prioritization of the NIST Framework's subcategories, agreed to by a diverse group of satellite industry experts, and can be used as a model by satellite industry members seeking to implement the Framework in their organization. Perhaps more important than the end product, in terms of managing cybersecurity risk, however, is the analytical process of identifying the scope of infrastructure components to be protected; examining the NIST Framework's recommendations in light of an organization's own priorities, capabilities, and vulnerabilities; and developing an implementation that is robust, self-reinforcing, and catered to the specific needs of an organization.

V. Illustrative Use Case

The following use case illustrates how the risk management principles of the NIST Cybersecurity Framework are implemented in the satellite segment on a day-to-day basis. This generic use case is based on actual incidents affecting commercial satellite communications systems, although specific facts have been omitted, revised, or consolidated for illustrative purposes and to protect classified or proprietary information. Although the use case is ordered according to the structure of the NIST framework, it also demonstrates how various risk management processes happen simultaneously and are mutually reinforcing.

A. Identify

Security personnel at satellite service providers constantly receive threat and vulnerability information from multiple sources, including industry information sharing forums, government channels, external databases of threat and vulnerability information (e.g., CERT Vulnerability Notes Database), published reports, and in-house security audits. (ID.RA-2). Information security roles and responsibilities are clearly defined within the

organization and communicated appropriately to external partners. (ID.GV-2). This includes designating points of contact within the service provider organization to receive threat information from partners. Additionally, communication and data flows within an organization are mapped and clearly understood, (ID.AM-3), ensuring that threat information, once communicated to an organization, is disseminated to the appropriate personnel to take protective action.

In the illustrative case, a security researcher identifies vulnerabilities in specific satellite user terminals with hardcoded login credentials and undocumented proprietary protocols for accessing device firmware. Satellite service providers learn of the vulnerabilities through their information collection mechanisms. For example, some affected service providers are notified through established channels of communication with the Computer Emergency Response Team (CERT) Coordination Center or the National Coordinating Center for Communications' (NCC) Information Sharing and Analysis Center (Comm-ISAC), both sponsored by DHS. Multiple industry groups, including the Satellite Industry Association (SIA) the Global VSAT Forum (GVF), and the Space Data Association (SDA), also disseminate the vulnerability information and facilitate coordination among industry members.

B. Protect

Protection mechanisms are in place to prevent vulnerabilities from developing, or to contain and mitigate the effect of any exploit. Satellite service providers implement multiple layers of security and separation within their systems to isolate and insulate critical infrastructure and services from the network edge and other non-mission critical enterprise systems. (PR.AC-5). Particularly relevant to this use case, system access is closely controlled and monitored, particularly for critical services. Identities and credentials are managed, (PR.AC-1), physical access to infrastructure assets is controlled (PR.AC-2), remote access is monitored, managed, and limited as appropriate, (PR.AC-3), and clear processes are in place to secure and control changes to infrastructure or user terminal configuration and firmware. (PR.IP-3).

In the case of the user terminal vulnerability, analysis of the threat (discussed in the context of the Detect function, below) reveals that some protections already in place mitigate the identified vulnerability. For example, some of the affected equipment can only be accessed physically or through the satellite service provider network's interconnection with the Internet. This limits the opportunities for exploiting the vulnerability and creates effective mechanisms for monitoring. In the airborne context, the satellite terminal is onboard an aircraft with multiple layers of mitigation and protection for the network that will prevent unauthorized access to the terminal, whether from an individual on the ground or even on the aircraft. For example, the affected terminal is contained in an electronics bay below the floor of the aircraft, inaccessible to anyone in the cabin.

C. Detect

Detection includes ongoing active monitoring of satellite communications systems and services to identify events and anomalies, (DE.CM-1), analysis of detected events to understand the target, methods, and mitigation opportunities (DE.AE-2), and an evaluation

of the impacts and consequences of a detected event. (DE.AE-4). Effective detection requires clearly defined roles and responsibilities within the security team and organization as a whole, to ensure that threats are detected and fully analyzed, and that information and practices developed through the Identify and Protect functions are appropriately leveraged. Depending on an organization's resources and Framework Implementation Tier, various scenarios might be run to determine the possible effect of an exploit of the vulnerability.

In the illustrative use case, the vulnerability information gained through the Identify function is analyzed in the context of existing controls, policies, and security features to evaluate the nature of the threat. It is determined that the vulnerability identified does not pose a serious threat to critical infrastructure because of multiple layers of protection that were in place. For example, the vulnerability is limited to user terminals and cannot affect central network functions. Additionally, in cases where physical proximity is required to exploit the vulnerability, there are additional layers of protection that decrease the likelihood of a serious exploit.

However, while the threat could not affect the critical infrastructure, there might be some potential for interference with individual units or communications sessions supporting critical services. As such, the satellite service providers begin appropriate measures to respond to the threat.

D. Respond

Response synthesizes the information and practices coming out of the Identify, Protect, and Detect functions to address and resolve an event effectively. Response begins when events identified through the Detect function are reported and prioritized consistent with established criteria. (RS.CO-2). Upon receiving the report, security personnel begin to analyze the vulnerability, assess its impact, and develop solutions. (RS.AN-1, RS.AN-2). During the course of executing a response, information about the threat and identified mitigation is shared internally among operational and security teams, (RS.CO-3), and appropriate coordination occurs with users, partners, and other stakeholders. (RS.CO-4). Ultimately, the goal of effective response is to contain an event, (RS.MI-1), and mitigate its effect (RS.MI-2). Response efforts should feed directly back into and strengthen the processes undertaken through the Identify, Protect, and Detect functions, in order to improve overall incident response and enterprise risk management. (RS.IM-1)

In the illustrative use case, service providers analyze the vulnerability information and develop a series of reactive and proactive steps to contain and mitigate the event. Reactively, service providers implement new mechanisms for detecting and blocking use of the hardcoded credentials at the points where the satellite system interconnects with public terrestrial networks, thereby blocking remote unauthorized use of the device. Security updates are made to device firmware, which are distributed to terminals through standard channels.

Proactively, service providers incorporate lessons learned into operational and security processes going forward. Companies with vulnerability models and other security tools for

systems they develop and deploy test those models against the event and revise them to improve protection.

Service providers also coordinate with numerous parties in the course of addressing the vulnerability. Service providers work with partners and equipment manufacturers to develop and deploy fixes for user terminals. Service providers also communicate with customers to make them aware of any required fix or changed practices. Because of the strong partnership between the satellite industry and its military and government customers, satellite providers communicate with government to ensure that questions are answered and needs are addressed. Response is also coordinated through third party mechanisms like CERT or industry bodies, to bolster the collective security knowledge base and improve overall security.

E. Recover

Recovery is the process of restoring any capabilities or services that were impaired due to an event and maintaining plans for incident response. For the satellite industry, this means ensuring that critical communications services are preserved or restored. It also involves improving protection, detection, and response efforts; for the satellite industry, continuous process improvement is incorporated as an essential aspect of each of the Framework functions.

In the illustrative use case, there is no detrimental effect on critical infrastructure or critical services, so limited recovery efforts are required. As the segment has been performing the other functions, it has been engaged in reflection and process improvement. Individual companies also communicate these lessons and measures throughout the industry and to customers, to assist in threat identification, protection, detection, and response going forward.

VI. Conclusion & Recommendations

- Satellite industry members should review this report and use the analytical process therein to adapt the NIST Framework approach to cybersecurity risk management to their own operations and networks. Industry members are invited to use the risk management matrix above as a starting point in adapting the NIST Framework, or to develop their own matrix, using the analytical process described in this report as a guide.
- Industry members should participate in multiple channels of information sharing. As described in the illustrative use case, robust collaborative efforts already are underway, both among industry, and between the public and private sectors. In addition to sharing vulnerability and solution information, industry members should ensure that they are communicating sufficiently internally and externally to deliver adequate assurances regarding their cyber security risk management practices.
- Continued flexibility is essential for use of the NIST Framework given the diversity within the satellite segment. As such, each satellite operator is best positioned to understand and address its cybersecurity risks, and each should be afforded flexibility to apply the framework to their network architecture.

- Industry members should ensure that the NIST Framework and the WG 4 report are disseminated throughout their organizations, in particular to management and staff with a security or IT function.

VII. Acknowledgments

The satellite segment acknowledges the substantial contributions of time and expertise from each of the individuals and companies represented on the subgroup.

The Segment also acknowledges the significant assistance and input from the other Segment and Feeder Subgroups within Working Group 4.

VIII. 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

CSRIC 2A Cybersecurity Best Practices
http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf

9.4 WIRELESS SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

CSRIC WORKING GROUP 4
WIRELESS SEGMENT REPORT

I. Executive Summary

The Wireless Segment is a subgroup within the CSRIC Working Group 4 effort and focused on wireless technology, networks and services as it relates to cybersecurity risk management and critical infrastructure. The Wireless Segment is comprised of industry experts in the fields of wireless and telecommunications.

In order to accomplish the foundational objectives laid out by the FCC, the wireless segment sought to conform to the NIST Cybersecurity Framework. While the NIST Framework may be used beyond critical infrastructure, the analysis was primarily focused on critical infrastructure as defined in the Cybersecurity Executive Order[46] (i.e. both physical and virtual).

The wireless segment conducted an assessment by developing a detailed representative profile focused on wireless critical infrastructure based on the DHS NSRA Model and existing threat information sharing models used within the Communications Sector. Nonetheless, individual companies will have to go through these steps for themselves to develop their own cyber risk management programs, applying the framework to their own circumstances.

II. Introduction

The Wireless Segment is a subgroup within the CSRIC Working Group 4 effort and is focused on wireless technology, networks and services as it relates to cybersecurity risk management and critical infrastructure.

The last set of comprehensive cybersecurity best practices was recommended by CSRIC III in March 2011. The wireless segment within CSRIC IV Working Group 4 evaluated CSRIC's most critical existing cybersecurity best practices and existing present day standards and best practices to determine how best to address alignment with the NIST Cybersecurity Framework and account for changes in cybersecurity practice and the threat landscape.

The Working Group will harmonize these best practices with current and up to date practices and the NIST Cybersecurity Framework, version 1.0. The Framework defines a taxonomy for managing cyber risk. The risk management process is defined in five functions, identify, protect, detect, respond, and recover (as described in Section IV below). The Framework represents a virtuous cycle of continuous improvement in cybersecurity. Depending on the size, scope of critical assets and services and maturity of an organization,

[46] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013) [hereinafter *EO 13636*].

the Framework may be adapted to meet organizational requirements.

III. Wireless Segment Group Members

Martin Dolly	AT&T
Kathy Whitbeck	Cellcom/Nsight
Joel Capps	Ericsson
Daniel Devasirvatham	Idaho National Labs (inl.gov)
Jesse Ward	NTCA
Karl Schimmeck	SIFMA (Securities Industry and Financial Markets Ass.
Chuck Brownawell	Sprint
Shellie Blakeney	T-Mobile
Harold Salters	T-Mobile
Danna Velsecchi	Verizon

IV. Background

Wireless networks consist of physical and logical entities that provide support for mobile network features and telecommunication services. The support provided includes functionality, for management of mobile devices information, control of network features and services, and the transfer (switching and transmission) mechanisms for signaling and for user generated information. The core network consists of both the circuit switched core network, which supports circuit switched services (e.g. voice), and the packet-switched core network, which supports IP-based packet services (See Section VI).

As outlined below, the wireless segment identified critical infrastructure assets and services pertinent to the core network. Consistent with the identified critical assets and services, existing threat information sharing models are used based on the DHS NSRA model and established practices[47] from a risk assessment and threat environment perspective to establish alignment priority with respect to the NIST Framework. The focus is on wireless network critical infrastructure and services as defined herein, as compared to practices or services that may exist to address consumer facing web services or portals.

V. Objective, Scope and Methodology

The foundational objectives of Working Group 4 include the following[48]:

- To conform the NIST Framework to the communications sector:- Identify core mission(s), critical infrastructure and risks to the communications sector and organize

[47] See Cellular Telephone Industries Association ('CTIA'), *Today's Mobile Cybersecurity Information Sharing* (2014), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf?sfvrsn=2.

[48] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management Best Practices (WG4)* (2014), *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-4_Report_061814.pdf.

the NIST core framework based on the aspects most relevant to ensuring the reliability and integrity of the core communications infrastructure.

- Maintain flexibility for individual companies. As part of this exercise, based on updated threat information, and consistent with the NIST Framework, the conformed communications sector framework will allow individual companies flexibility to self-determine how to apply the framework to their business based upon their individual risk profile, risk tolerance, and critical infrastructure ownership.

- Develop new streamlined practices that align with the Framework's organization and common risk management approaches. Use existing CSRIC Best Practices and other resources to inform and organize the Framework with the goal of providing companies with a "guide" of communication segment specific practices that companies may elect to implement to mitigate cyber risk.

- Develop use cases/examples of how the framework is being used within the sector. Develop an appendix with illustrative examples or use cases about how the framework is being used or incorporated into risk management processes of communications companies. Descriptions will be anonymized and provide examples that could be considered by all sectors regarding how aspects of the framework could be voluntarily used.

- Provide guidance to incorporate the framework into existing company risk management processes. Determine high level processes that companies could perform, to the extent they use the framework, to incorporate it into their existing risk management program, or build a cyber-risk management program where none exists today.

The NIST Framework itself suggests seven steps to using the framework and affords firms the flexibility to apply those steps unique to their business situation. With respect to the wireless segment, those steps include[49]:

- **Step 1: Prioritize and Scope**. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

- **Step 2: Orient**. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets,

[49] *See* National Institute for Standards and Technology, *Framework for Improving Cybersecurity* (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [hereinafter *NIST CSF*].

regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

- **Step 3: Create a Current Profile**. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

- **Step 4: Conduct a Risk Assessment**. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

- **Step 5: Create a Target Profile**. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

- **Step 6: Determine, Analyze, and Prioritize Gaps**. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

- **Step 7: Implement Action Plan**. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

In order to accomplish the foundational objectives laid out by the FCC, the wireless segment developed a sample "voluntary" profile to aid companies in the application of the framework to their business. Given that the NIST Framework, while it may be used beyond critical infrastructure, was primarily focused on critical infrastructure, the wireless sub-group started its assessment by developing a detailed representative profile focused on

wireless critical infrastructure. The purpose of this document is to provide recommendations regarding how to best apply the framework. Individual companies will have to go through these steps for themselves to develop their own cyber risk management programs, applying the framework to their own circumstances.

In order to prioritize the NIST Framework best practices, the wireless segment collaborated with other segment teams (e.g. wireline) to review and provide input on a standard worksheet that considered the best practices according to a variety of factors. These factors included considering whether each functional area, category and sub-category were in or out of scope, how they may be applied, their criticality to protecting against cyber threats, and difficulty to implement. The working group also considered a variety of factors in making these determinations including several barriers to entry including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers. Finally, as part of the criticality assessment, the wireline segment considered the various threats that were outlined by the Threats Feeder Group. This analysis enabled the team to categorize the various functional areas, categories and sub-categories into three buckets of practices: highest priority, mid-tier and tertiary priority (as outlined in Section VI below).

VI. Results & Findings: Wireless Segment

In order to create a sample profile, the wireless segment first reviewed the NIST Framework in the context of critical infrastructure. The framework could also be viewed for other factors beyond critical infrastructure consistent with each individual sector or company's priorities and core mission applying the seven steps outlined by NIST as discussed above.

In developing a representative profile for critical infrastructure the segment considered critical infrastructure consistent with the definition discussed in President Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity" which states that critical infrastructure includes those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[50]

Further, in 2012 the Communications Sector, in partnership with DHS, completed the 2012 Risk Assessment for Communications (referred to going forward as the National Sector Risk Assessment or NSRA), updating its 2008 report ,which assessed physical and cyber threats to the communications infrastructure. The risk assessment was intended to further the goals of the Communications Sector Specific Plan, also developed jointly with DHS in 2010, to identify and protect national critical network components, ensure overall network reliability, maintain "always-on" service for critical customers and quickly restore critical communications functions and services following a disruption. The wireless segment

[50] *See EO 13636*.

agreed that the scope of the efforts in Working Group 4 should build upon the work already completed in the 2012 risk assessment.

The 2012 risk assessment proposes an architectural model that effectively divides the communications network infrastructure into three components between (1) services and applications, (2) the core network and (3) access networks.

The 2012 NSRA assessed the risk to the communications infrastructure from both physical and cyber-attacks. Specifically, the Communications Sector determined the risks from single cyber incidents could result in the loss of network confidentiality, integrity, or availability. However, the conclusion of the 2102 NSRA was that these impacts were largely limited to a small portion of the network infrastructure. Based upon this analysis, the sector determined that while the sector's "wireless access segments are vulnerable to single incidents; most risks would be limited to a local or regional area and would not result in national communications disruptions and/or outages". The sector identified some exceptions, including one specific to the "core network that could result in national communications disruptions and/or outages: malicious actors committing resource exhaustion against multiple core network components of a particular make/model". In addition there may be other critical infrastructure sectors that may use wireless at the regional level e.g. Energy Sector, and cross sector efforts work to evaluate impacts where possible.

The Communications NSRA architecture model (see Figure below) identifies national level communications architecture elements that are at elevated risk and serves as a baseline to prioritize the communications infrastructure.

Figure 2-2 from the 2012 risk assessment illustrates the NSRA architectural model:

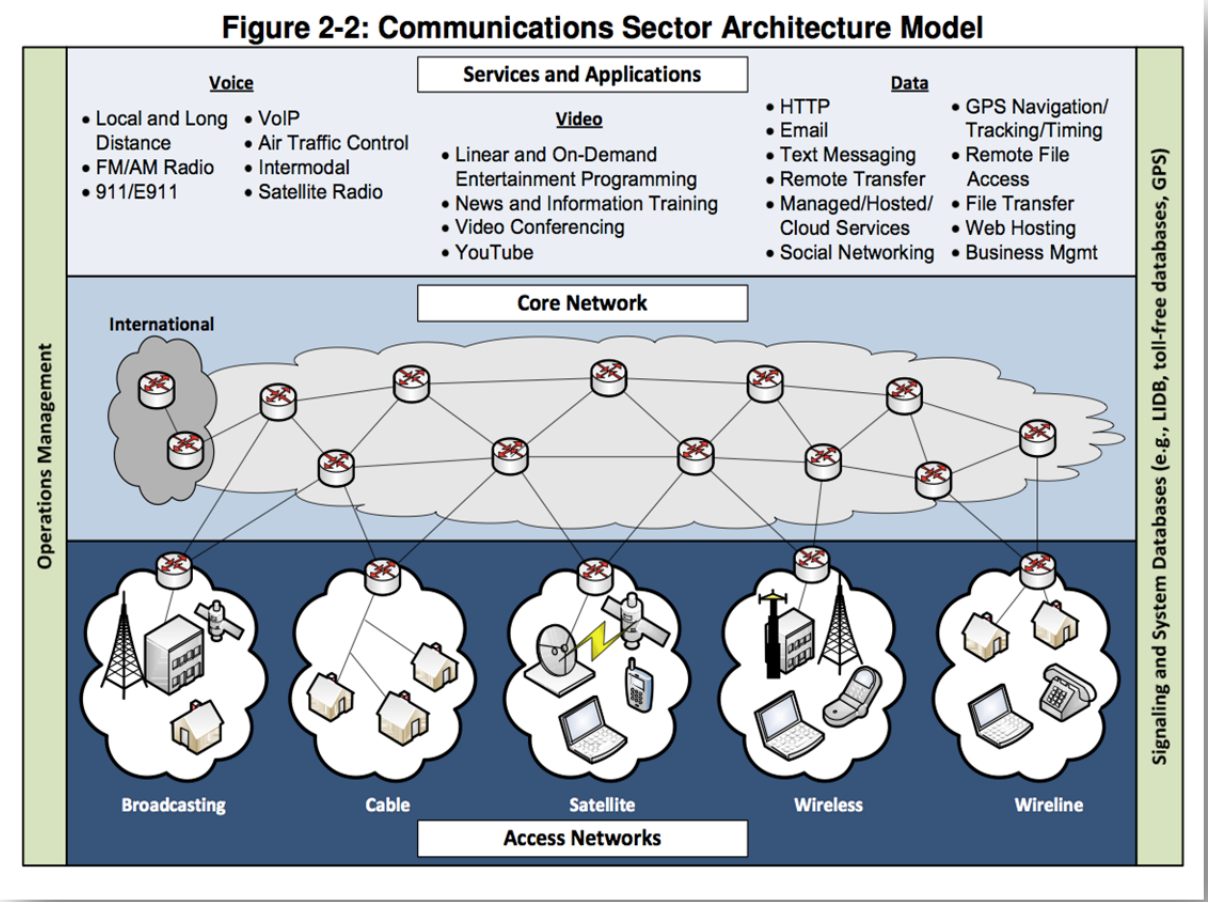
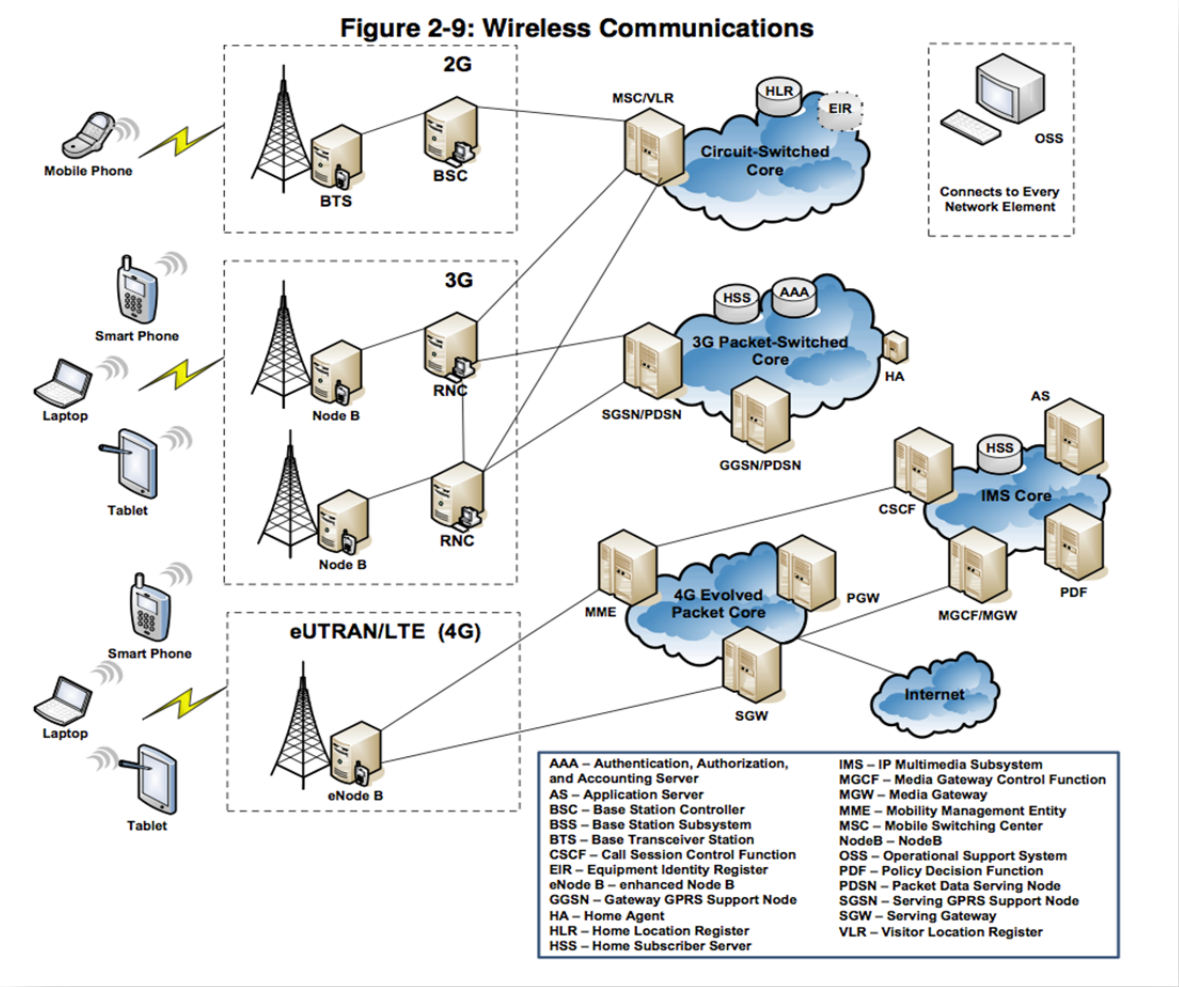


Figure 2-9 illustrates the NSRA Model that the Wireless Segment Specific Model is based on:



Based on the NSRA Wireless Communications Model and the definition of Critical Infrastructure contained in Executive Order 13636[51] **the following elements and services are considered critical for purposes of the scope of this Segment report.** The elements shown below are functional descriptions that correspond to the elements shown in the model (e.g. Location Registers correspond to Home Location Register and Visitor Locations Register) for purposes of being technology neutral and to focus on the critical function/asset or service.

The focus of this report is based on the NSRA Model for the critical assets and services identified in below as it relates to the NIST CSF. However, it is important to note that the CSF can readily be applied beyond what is identified below and provides the flexibility for each organization to determine their needs as identified by a risk based cybersecurity assessment.

A. Areas of Critical Focus or Assets

As outlined below the wireless segment identified critical infrastructure assets and services. Consistent with the identified assets and services, existing threat information sharing models are used to coordinate among sector participants based on the DHS NSRA model and established practices[52] from an overall risk assessment and threat environment that is dynamic and constantly changing. The information sharing practices address wireless network critical infrastructure and services as defined herein, as compared to practices or services that may exist to address consumer facing web services or portals.

1) Location Registers

Location Registers are used to provide mobility functions within the mobile network based on location information associated with the mobile device. Typical Location Registers are described in the 3GPP Standards[53] and others[54] as the Home Location Register (HLR) and Visitor Location Register (VLR). The Home Location Register (HLR) is the main database of permanent subscriber information for a mobile network. Maintained by the subscriber's home carrier, the HLR contains pertinent user information, account status, and preferences. The HLR interacts with the other elements in the mobile core network for call control and processing. Another example Location Registers is the Visiting Location Register (VLR), which maintains temporary user information (such as current location) to manage requests from devices that are out of the area covered by the home system.

---

[51] *See EO 13636*.
[52] *See* Cellular Telephone Industries Association ('CTIA'), *Today's Mobile Cybersecurity Information Sharing* (2014), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf?sfvrsn=2.
[53] *See* Third Generation Partnership Project (3GPP), http://www.3gpp.org (last visited Mar. 13, 2015).
[54] *See* Alliance for Telecommunications Industry Solutions, http://www.atis.org (last visited Mar. 13, 2015); *See* 3rd Generation Partnership Project 2, http://www.3gpp2.org (last visited Mar. 13, 2015); *See* Telecommunications Industry Association, http://www.tiaonline.org (last visited Mar. 13, 2015).

2) Identity and Authentication Registers

Identity and device authentication are basic and fundamental functions to the proper and reliable operation of the mobile network. The device identity and authorization to access mobile network services are critical to ensure proper functioning of mobile services. Examples of registers that correspond to these critical elements may be found in 3GPP and other Standards, and are often referred as the HSS (Home Subscriber Server). The HSS is a central database that contains user-related and subscription-related information. The functions of the HSS include functionalities such as mobility management, call and session establishment support, authentication and access authorization. Other examples of Identity Registers include the Authentication Center (AuC) and may be found in 3GPP and other mobility Standards.

3) Mobile Switching & Packet Core Entities

The Mobile Switching and Packet Core Entities are elements of the mobile network that carry out call switching functions for mobile devices roaming on the network of base stations. It allows mobile devices to communicate with each other and telephones in the wider public switched telephone network (PSTN) or across the Internet to Websites, Applications and other resources available through the Internet. The architecture contains specific mobile capabilities and functions which are needed because mobile devices are not fixed in one location.
Originally the mobile core network consisted of the circuit-switched core network, used for traditional services such as voice calls, SMS, and circuit switched data calls. The packet core functions extended the architecture to provide packet-switched data services and Internet connectivity.

4) Mobility Management Core Entity

Mobility Management is one of the major functions that allow mobile devices to work properly. The Mobility Management Core Entity is a key control-node and is involved in such functions as the bearer activation/deactivation process and is also responsible for choosing how devices attach to the mobile network and the control of temporary identities. The functionality is detailed in 3GPP and other mobile Standards.

5) Core Signaling Entities (Common with Wireline and possibly other segments)

The Core Signaling Entities correspond to those elements that provide signaling control and services functions that provides for coordination, reliability and authentication to the core functions such as the Location Registers, Identity and Authentication Registers, Mobile Switching and Mobility Management Core entities. Signaling System No. 7 (SS7), the ISDN User Part (ISUP), the GSM-Mobile Application Part (GSM-MAP), and ANSI-41 are examples of protocols that may be used by Core Signaling entities.

6) Core Policy Entities (Common with Wireline and possibly other segments)

The Core Policy Entities correspond to those elements that provide policy control functions that provides for coordination, reliability and authentication to other mobile network core functions such as the Mobility Management Core entities. RADIUS and DIAMETER[55] are examples of protocols that may be used by Core Policy entities.

B. Critical Services

1) Network Availability

With more mobile devices available than the number of people in the United States, mobile network availability to end-users is of utmost importance and has become critical to ensuring communications, particularly during natural disasters and other emergencies. The critical functions of the mobile core network as identified by the NSRA, place network availability and reliability as the highest priority and support the critical services outlined below.

2) Wireless Emergency Alerts[56] (WEA) - (National mobile messaging alert capability that appears on a mobile device similar to a text message, but there are two fundamental differences:

- WEA use a different kind of technology to ensure these alert messages are delivered immediately and are not subject to potential congestion (or delays) on wireless networks.
- WEA use a point-to-multipoint system, which means alert messages will be sent to mobile users within a targeted area, unlike text messages which are not location aware. For example, if a Washington, D.C. mobile user has a WEA-capable device, but happened to be in an area in southern California when an earthquake occurred, the device would receive an "Imminent Threat Alert."

[55] *See* Wikipedia, *Diameter (protocol)*, http://en.wikipedia.org/wiki/Diameter_%28protocol%29 (last visited Mar. 13, 2015); *See* Wikipedia, *RADIUS*, http://en.wikipedia.org/wiki/RADIUS (last visited Mar. 13, 2015).
[56] See Cellular Telephone Industries Association, *Wireless Emergency Alerts*, http://www.ctia.org/your-wireless-life/consumer-tips/wireless-emergency-alerts (last visited Mar. 13, 2015).

3) Enhanced 911, E-911 or E911, and NG911

The mobile network is part of a system that links emergency callers with the appropriate public resources commonly referred to as a Public Safety Answering Point (PSAP). A mobile device, regardless of whether or not it is provisioned on a network, has the ability to support a call when the user calls the digits "911". In addition to voice communications, text communications are also being rolled out in States[57]. Next Generation 911 (NG911) enables the public to obtain emergency assistance by means of advanced communications technologies beyond traditional voice-centric devices, or send additional information of an incident including pictures and videos.

4) Wireless Priority Services (WPS)

WPS is a voluntary DHS program that supports national leadership; Federal, State, local, tribal and territorial governments; and other authorized national security and emergency preparedness users. It is intended to be used in an emergency or crisis situation when the wireless network may be congested and the probability of completing a normal call may be reduced. It also requires the mobile device to access the wireless channel before the call is prioritized.

a. Government Emergency Telecommunications Service (GETS)
Government Emergency Telecommunications Service (GETS) supports national leadership; Federal, State, local, tribal and territorial governments; and other authorized national security and emergency preparedness (NS/EP) users. It is intended to be used in an emergency or crisis situation when the landline network is congested and the probability of completing a normal call is reduced.

C. Alignment with NIST Cybersecurity Framework

This document will assist participants in the wireless segment to align with the NIST Cybersecurity Framework by tailoring the framework's categories and subcategories to best serve the segment's unique cybersecurity challenges and provide use cases, which will highlight how to apply a risk evaluation and mitigation process.

1) Functions

Based on the NIST Cybersecurity Framework and the Five Functions specified in the document, the wireless segment deemed the following to be relevant to the critical elements and services identified above.

[57] See Federal Communications Commission, *Best Practices for Implementing Text-to-911* (2014), *available at* www.fcc.gov/encyclopedia/best-practices-implementing-text-911.

i. Identify

The Identify Function seeks to identify the business context and resources necessary to support functions which are critical, enabling organizations to prioritize and focus efforts.

The following are the key components of the Identify Function:

a. **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.
b. **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
c. **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
d. **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
e. **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ii. Protect

The Protect Function is the first line of defense, implemented through a range of security controls and procedures that implement policies resulting from the Identify Function.

The following are the key components of the Protect Function:

a. **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
b. **Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
c. **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
d. **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities,

management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

e. **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
f. **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

iii. Detect

The expectation is that security policies may have gaps or that security controls may be imperfect, resulting in occasional security incidents. These incidents must be detected to be effectively managed, and the Detect Function seeks to accomplish that.

The following are the key components of Detect Function:

a. **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
b. **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
c. **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

iv. Respond

Once a security incident has been detected, a response is required to remediate the incident, which is the goal of the Respond Function.

The following are the key components of Respond Function:

a. **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
b. **Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.
c. **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
d. **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

v. Recover

While the respond phase seeks to address an individual security incident, the recovery seeks to update security policies and controls within the Protect Function to ensure future attacks of the same type are not successful.

The following are the key components of Recovery Function:

a. **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
b. **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.
c. **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs[58], and vendors.

2) Relevant Categories

The categories and subcategories below, taken from the NIST Cybersecurity Framework (CSF), Version 1.0 represent different levels of risk management activities along a continuum from large to medium and small sized organizations. As outlined in the CSF an organization can use the categories and subcategories as a key part of a systematic process for identifying, assessing, and managing cybersecurity risk. The categories and subcategories are tools that an organization can use to determine activities that are most important to critical assets and services. For purposes of this document the tables below relate to the critical assets and services identified above.

This document purposely ***does not*** define Large, Medium and Small sized organizations; however, with respect to possible examples of the large organizational case the following may be considered:

A large sized organization may be an owner/operator of most, if not all of the critical assets and services outlined above and may have a national footprint in terms or geographic coverage, subscriber base and operations overall.
The purpose of using organization size below is to help guide and prioritize categories and subcategories given the flexibility in the CSF to scale. Individual owner/operators of the critical assets and services identified above may determine, on a case by case basis which categories and subcategories are in-scope and most relevant to their specific situation and risk management process.

NOTE: Analysis of Medium and Small sized organizations has been assigned to the SMB Sub-group within Working Group 4 and is intentionally not reflected below.

[58] *See* CSIRT, https://www.csirt.org/ (last visited Mar. 13, 2015).

i. Identify Function

Function & Categories	Organization Size & Scope	Relevant Categories
Identify	Large **Out-of-Scope (see below):** **ID.AM-3** **ID.AM-6**	**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.
	Large **Out-of-Scope (see below):** **ID.BE-1** **ID.BE-3**	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Large	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Large **Out-of-Scope (see below):** **ID.RA-4**	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Large	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ii. Protect Function

Function & Categories	Organization Size & Scope	Relevant Categories
Protect Function	Large	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Large	**Awareness and Training (PR.AT):** The organization's personnel and **partners** are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies,

		procedures, and agreements.
	Large	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Large **Out-of-Scope (See below):** **PR.IP-2** **PR.IP-11**	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Large	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Large	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

iii. Detect Function

Function & categories	Organization Size & Scope	Relevant Categories
Detect Function	Large	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Large	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

	Large **Out-of-Scope (See below):** **DE.DP-4**	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

iv. Respond Function

Function & Categories	Organization Size & Scope	Relevant Categories
Respond Function	Large, Medium, Small	**Communications (RS.RP):** Response process and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Large **Out-of-Scope (See below):** **RS.CO-4**	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Large	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.
	Large	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Large	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

v. Recover Function

Function & Categories	Organization Size & Scope	Relevant Categories
Recover Function	Large	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Large	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Large **Out-of-Scope (see below):** **RC.CO-1** **RC.CO-2** **RC.CO-3**	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Note: In the Scoping Analysis that follows below, both Wireline and Wireless Sub-Groups are referenced because the analysis was conducted jointly by the two Sub-Groups and is the same for both. There is no intention to address the Wireline Segment in this report. The material contained in the report herein is solely focused on the Wireless Segment analysis.

SCOPING ANALYSIS

	In Scope/Out of Scope	Application
	Wireless & Wireline Sub-Groups	**Wireless & Wireline Sub-Groups**
Sub-Category	Is the function, category, sub-category in scope as a best practice for the critical infrastructure "systems and assets" determined by the sub-group (aligned wireless & wireline)? (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).
ID.AM-1: Physical devices and systems within the organization are inventoried	In Scope	Applies to core infrastructure elements
ID.AM-2: Software platforms and applications within the organization are inventoried	In Scope	

	In Scope/Out of Scope	Application
ID.AM-3: Organizational communication and data flows are mapped	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
ID.AM-4: External information systems are catalogued	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	In Scope	
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Out of Scope	Only relates to a company's overall business risk management program not impacting the operability of critical infrastructure
ID.BE-1: Organization's role in the supply chain is identified and communicated	Out of Scope	Related to Enterprise IT or overall corporate function
ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated	In Scope	Helps organizations understand their role in the industry and impact on cybersecurity.
ID.BE-3: Priorities for organizational mission, objectives and actives are established and communicated	Out of Scope	Related to Enterprise IT or overall corporate function

	In Scope/Out of Scope	Application
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	In Scope	See ID-BE2
ID.BE-5: Resilience requirements to support delivery of critical services are established	In Scope	
ID.GV-1: Organizational information security policy is established	In Scope	Related to security around critical components and infrastructure
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	In Scope	Smaller organizations may not have multiple groups
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.GV-4: Governance and risk management processes address cybersecurity risks	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.RA-1: Asset vulnerabilities are identified and documented	Rephrase - Asset vulnerabilities and threats are identified	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above

	In Scope/Out of Scope	Application
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.RA-3: Threats, both internal and external, are identified and documented	Rephrase - Asset vulnerabilities and threats are documented	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.RA-4: Potential business impacts and likelihoods are identified	Out of Scope	Related to business risk not the operability of critical infrastructure
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.RA-6: Risk responses are identified and prioritized	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	In Scope - only for personnel that work with critical infrastructure assets….	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above

	In Scope/Out of Scope	Application
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	In Scope - same as above	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AC-1: Identities and credentials are managed for authorized devices and users	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AC-2:Physical access to assets is managed and protected	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AC-3:Remote access is managed	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AT-1: All users are informed and trained	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above

	In Scope/Out of Scope	Application
PR.AT-2: Privileged users understand roles & responsibilities	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AT-3: Third-party stakeholders (e.g., suppliers customers, partners) understand roles & responsibilities	In Scope	Only related to issues related to or impacting the physical devices or systems associated with the critical infrastructure inventoried above
PR.AT-4: Senior executives understand roles & responsibilities	Only senior executives that are responsible for overseeing critical infrastructure	
PR.AT-5: Physical and information security personnel understand roles and responsibility	Only information security personnel that are responsible for overseeing critical infrastructure	
PR.DS-1: Data-at-rest is protected	In Scope	Only as related to critical infrastructure
PR.DS-2: Data-in-transit is protected	In Scope	Only as related to critical infrastructure
PR.DS-3: Assets are formally managed throughout removal, transfers and disposition	In Scope	Only as related to critical infrastructure
PR.DS-4: Adequate capacity to ensure availability is maintained	In Scope	Only as related to critical infrastructure
PR.DS-5: Protections against data leaks are implemented	In Scope	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	In Scope	Only as related to critical infrastructure
PR.DS-7: The development and testing environment(s) are separate from the production environment	In Scope	Only as related to critical infrastructure
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	In Scope	Only as related to critical infrastructure
PR.IP-2: A System Development Life Cycle to manage systems is implemented	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
PR.IP-3: Configuration change control processes are in place	In Scope	Only as related to critical infrastructure
PR.IP-4: Backups of information are conducted, maintained and tested periodically	In Scope	Only as related to critical infrastructure
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	In Scope	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
PR.IP-6: Data is destroyed according to policy	In Scope	Only as related to critical infrastructure
PR.IP-7: Protection processes are continuously improved	In Scope	Only as related to critical infrastructure
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	In Scope	Only as related to critical infrastructure
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	In Scope	Only as related to critical infrastructure
PR.IP-10: Response and recovery plans are tested	In Scope	Only as related to critical infrastructure
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
PR.IP-12: A vulnerability management plan is developed and implemented	In Scope	Only as related to critical infrastructure
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	In Scope	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	In Scope Duplicative w/ AC-	Only as related to critical infrastructure
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	In Scope	Only as related to critical infrastructure
PR.PT-2: Removable media is protected and its use restricted according to policy	In Scope	Only as related to critical infrastructure
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	In Scope Duplicative w/ AC-4	Only as related to critical infrastructure
PR.PT-4: Communications and control networks are protected	In Scope	Only as related to critical infrastructure
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	In Scope	Only as related to critical infrastructure
DE.AE-2: Detected events are analyzed to understand attack targets and methods	In Scope	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	In Scope	Only as related to critical infrastructure
DE.AE-4: Impact of events is determined	In Scope	Only as related to critical infrastructure
DE.AE-5: Incident alert thresholds are established	In Scope	Only as related to critical infrastructure
DE.CM-1: The network is monitored to detect potential cybersecurity events	In Scope	Only as related to critical infrastructure
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	In Scope	Only as related to critical infrastructure
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	In Scope	Only as related to critical infrastructure
DE.CM-4: Malicious code is detected	In Scope out of scope in transport - malicious code targeting comms. infrastructure is in scope. Related back to PR-DR 6	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
DE.CM-5: Unauthorized mobile code is detected	In Scope Client Server vs. critical infra	Only as related to critical infrastructure
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	In Scope	I.e. switch manufacturer's remote diagnostic and or maintenance work.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	In Scope	Only as related to critical infrastructure
DE.CM-8: Vulnerability scans are performed	In Scope	Only as related to critical infrastructure
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	In Scope	Only as related to critical infrastructure
DE.DP-2: Detection activities comply with applicable requirements	In Scope	Only as related to critical infrastructure
DE.DP-3: Detection processes are tested	In Scope	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
DE.DP-4: Event detection information is communicated to appropriate parties	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
DE.DP-6: Detection processes are continuously improved	In Scope	Only as related to critical infrastructure
RS.RP-1: Response plan is executed during or after an event	In Scope	Only as related to critical infrastructure
RS.CO-1: Personnel know their roles and order of operations when a response is needed	In Scope	Only as related to critical infrastructure
RS.CO-2: Events are reported consistent with established criteria	In Scope	Only as related to critical infrastructure
RS.CO-3: Information is shared consistent with response plans	In Scope	Only as related to critical infrastructure
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	In Scope	Only as related to critical infrastructure

	In Scope/Out of Scope	Application
RS.AN-1: Notifications from detection systems are investigated	In Scope	Only as related to critical infrastructure
RS.AN-2: The impact of the incident is understood	In Scope	Only as related to critical infrastructure
RS.AN-3: Forensics are performed	In Scope	Only as related to critical infrastructure
RS.AN-4: Incidents are categorized consistent with plans	In Scope	Only as related to critical infrastructure
RS.MN-1: Incidents are contained	In Scope	Only as related to critical infrastructure
RS.MN-2: Incidents are mitigated	In Scope	Only as related to critical infrastructure
RS.MN-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	In Scope	Only as related to critical infrastructure
RS.IM-1: Response plans incorporate lessons learned	In Scope	Only necessary if response plan failed to contain or mitigate.
RS.IM-2: Response strategies are updated	In Scope	Only necessary if response plan failed to contain or mitigate.
RC.RP-1: Recovery plan is executed during or after an event	In Scope	Only as related to critical infrastructure
RC.RP-2: Recovery strategies are updated	In Scope	Only necessary if response plan failed to contain or mitigate.

	In Scope/Out of Scope	Application
RC.CO-1: Public related are managed	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
RC.CO-2: Reputation after an event is repaired	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	Out of Scope	Business management process not associated with ensuring the operability of critical infrastructure

Based on the Scoping Analysis shown above a further analysis of prioritizing the various in-scope subcategories was conducted. The analysis considered prioritization based on a scheme of Top Priority, Mid-Tier Priority and Tertiary Priority. Organizations may consider different schemes, but the analysis below illustrates an example of how to do so.

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 requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained
ID.RA-1: Asset vulnerabilities are identified and documented	ID.RA-6: Risk responses are identified and prioritized	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
PR.AC-1: Identities and credentials are managed for authorized devices and users	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties
PR.AC-2:Physical access to assets is managed and protected	PR.AT-2: Privileged users understand roles & responsibilities	DE.CM-5: Unauthorized mobile code is detected

Top Priority Subcategories	Mid-Tier Priority Subcategories	Tertiary Priority Subcategories
PR.AC-3:Remote access is managed	PR.AT-3: Third-party stakeholders (e.g., suppliers customers, partners) understand roles & responsibilities	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties	PR.AT-4: Senior executives understand roles & responsibilities	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	PR.AT-5: Physical and information security personnel understand roles and responsibility	DE.DP-3: Detection processes are tested
PR.DS-4: Adequate capacity to ensure availability is maintained	PR.DS-1: Data-at-rest is protected	RS.AN-3: Forensics are performed
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	PR.DS-2: Data-in-transit is protected	RS.AN-4: Incidents are categorized consistent with plans
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	PR.DS-3: Assets are formally managed throughout removal, transfers and disposition	RS.IM-1: Response plans incorporate lessons learned
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	PR.DS-5: Protections against data leaks are implemented	RS.IM-2: Response strategies are updated
PR.PT-4: Communications and control networks are protected	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	RC.RP-1: Recovery plans incorporate lessons learned
DE.CM-1: The network is monitored to detect potential cybersecurity events	PR.DS-7: The development and testing environment(s) are separate from the production environment	RC.RP-2: Recovery strategies are updated
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	PR.IP-3: Configuration change control processes are in place	
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	PR.IP-4: Backups of information are conducted, maintained and tested periodically	
DE.CM-4: Malicious code is detected	PR.IP-6: Data is destroyed according to policy	

Top Priority Subcategories
RS.RP-1: Response plan is executed during or after an event
RS.MN-1: Incidents are contained
RS.MN-2: Incidents are mitigated
RC.RP-1: Recovery plan is executed during or after an event

Mid-Tier Priority Subcategories
PR.IP-7: Protection processes are continuously improved
PR.IP-10: Response and recovery plans are tested
PR.IP-12: A vulnerability management plan is developed and implemented
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2: Removable media is protected and its use restricted according to policy
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
DE.AE-2: Detected events are analyzed to understand attack targets and methods
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
DE.AE-4: Impact of events is determined
DE.AE-5: Incident alert thresholds are established
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.CM-8: Vulnerability scans are performed
DE.DP-2: Detection activities comply with applicable requirements
DE.DP-6: Detection processes are continuously improved

Tertiary Priority Subcategories

Top Priority Subcategories	Mid-Tier Priority Subcategories	Tertiary Priority Subcategories
	RS.CO-1: Personnel know their roles and order of operations when a response is needed	
	RS.CO-2: Events are reported consistent with established criteria	
	RS.CO-3: Information is shared consistent with response plans	
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	RS.AN-1: Notifications from detection systems are investigated	
	RS.AN-2: The impact of the incident is understood	
	RS.MN-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	

The methodology used to arrive at the priority categories shown above was based on the determination of critical assets and services as described earlier in this section. From the defined assets and services the NIST Framework categories and subcategories were individually studied and assessed within the context of the risk based processes outlined below. The Risk Based Processes provides guidance on how an organization may consider prioritization of the subcategories to suit their situation and risk management needs.

D. Risk Based Processes

Historically, cybersecurity risk has been managed through compliance-based approaches. A security policy, whether developed internally or levied externally by a regulatory entity, informs technical and non-technical security controls that seek to reduce the probability and impact of intrusions (see Figure 6-1 below on left). In a compliance-based approach to cybersecurity, metrics focus on measuring the level of policy compliance, rather than the inherent risk. Compliance is often measured as a collection of binary outcomes, representing how many “check boxes” are “checked off”.

Figure 6-1. Compliance Approach

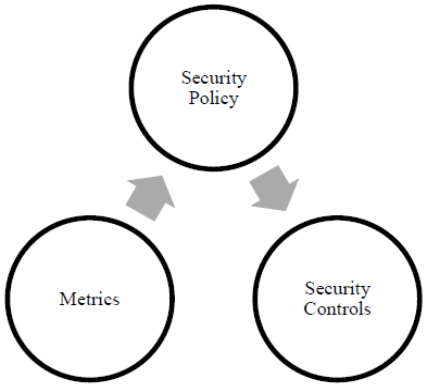
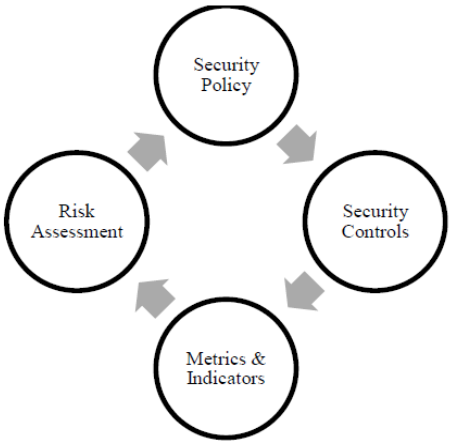
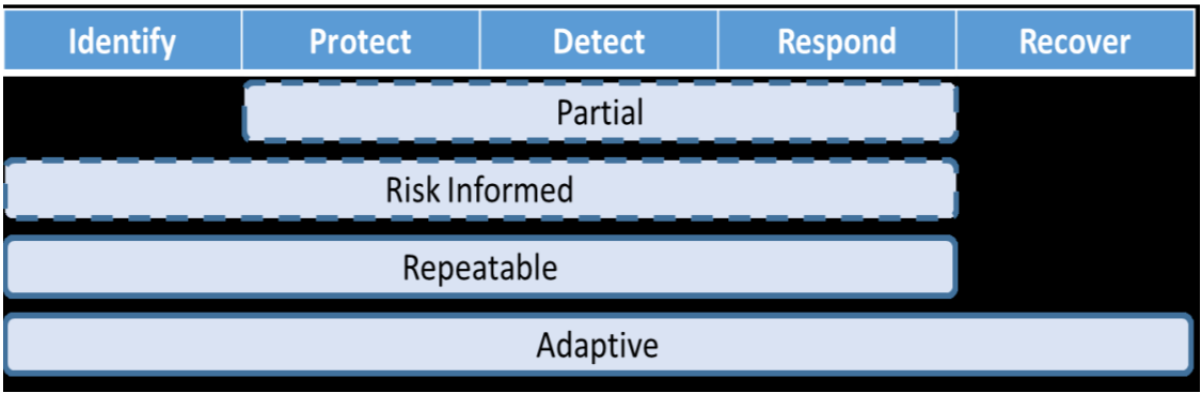


Figure 6-2. Risk-based Approach



Risk-based cybersecurity is a closed-loop cycle or process (see Figure 6-2 above on right). Security policies define what is and is not acceptable in an enterprise. These policies are enforced by both technical and non-technical security controls. Risk indicators are established. Based on the trends of these indicators, risk assessments are undertaken that trade off the cost/risk of intrusions against the cost/complexity of implementation and seek to modify security policies based on an informed risk assessment. From here the virtuous cycle repeats. The NIST Framework identifies the relevant Functions, Categories and Subcategories that may be used to implement the closed-loop cycle, and how an organization may improve over time and repetition of the cycle leading to improvement and process integration.



The level of risk management process integration within the NIST Framework is broken down into four tiers, and mapped against the Functions.

- **Partial:** There are no formal procedures in place and risk is managed in an ad hoc and reactive manner based on identified incidents.
- **Risk Informed:** Organizationally, cybersecurity risk is understood and security controls are deployed based on risk-informed, management-approved processes and procedures, but recovery and communications procedures are not well defined.
- **Repeatable:** A risk-informed approach is repeatable within the organization ensuring the ability to mitigate threats as they occur.
- **Adaptive:** Leading indicators are used to identify new types of threats and deploy protections in anticipation of an incident.

The following risk-based processes are described in the context of the critical assets and services identified above and Figure 6-2 above.

Commonly Used Processes:

1. Risk Assessment
2. Establish Cybersecurity Program
3. Review of Cybersecurity Practices
    a. Standards
    b. Procedures
    c. Controls
4. Risk Governance and Audit
5. Awareness and training
6. Anomalous activity detection and assets monitoring
7. Response activities and information sharing methods and procedures

VII. Illustrative Generic Use Case

Note: *Use cases associated with small and medium sized organizations are assigned to the SMB Subgroup within Working Group 4 and are not reflected in this document.*

Large Organizational Use Case

Definitions and Assumptions:

As defined in Executive Order 13636 Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The definition is taken from section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c (e)).

For the use case below the assumption is for a large sized organization. This document purposely ***does not*** define Large, Medium and Small sized organizations; however, with respect to possible examples the following may be considered for a large sized organization. Such an organization may be an owner/operator of most, if not all of the critical assets and services outlined in Section VI above and may have a national footprint in terms or geographic coverage, subscriber base and operations overall.

a. Critical Systems & Assets (See Section VI)
For this particular use case all of the assets from Section VI are assumed as part of the overall network configurations. Specifically the following are included:

1. Location Registers,
2. Identity & Authentication Registers,
3. Mobile Switching & Packet Core Entities,
4. Mobility Management Core Entity,
5. Core Signaling Entities, and
6. Core Policy Entities.

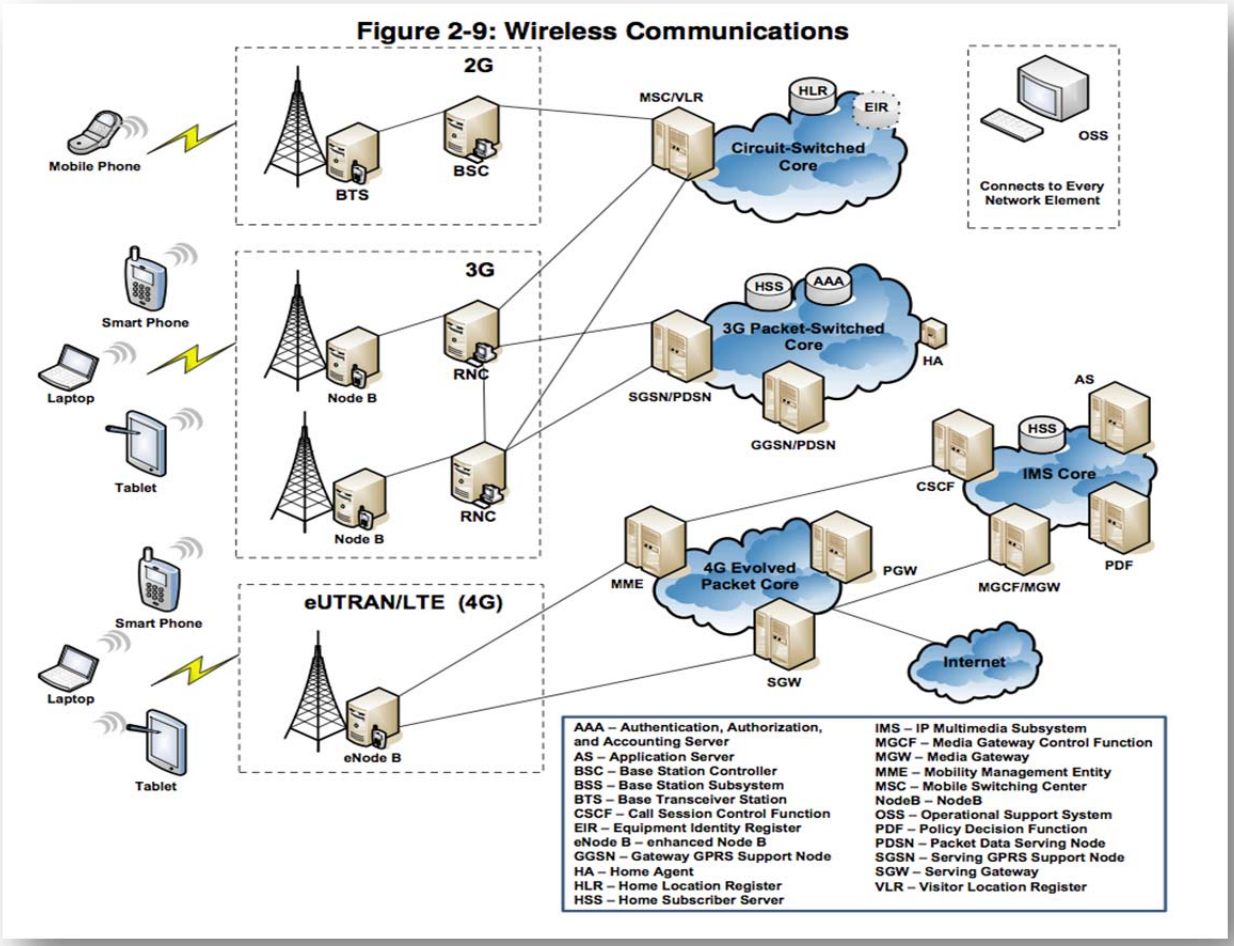
b. Critical Services (Virtual Assets & Systems) (See Section VI)
For this particular use case all of the services from Section VI are assumed as part of the overall network configurations. Specifically the following are included:

1. Network Availability
2. Wireless Emergency Alerts
3. Enhanced 911 & NG 911
4. Wireless Priority Services
5. GETS

c. Assumed Configuration

The assumed configuration is that shown below as outlined in the NSRA model from Section VI. It is replicated below for convenience.

Figure 2-9: Wireless Communications



d. Scope
In the general case of a large organization, i.e. operator/owner of critical infrastructure, national scope of all 50 States is assumed, as well as coverage of a significant portion of the US population. National coverage of 50 States may be accomplished through roaming partner capabilities in addition to those assets and services provided by the owner/operator.

e. Threat Impacts

i. Systems & Assets – Disruption of network availability for wireless communications nationally would have a debilitating impact on public confidence and well-being, security, national economic security, and public safety.

Part of network availability includes the capability for consumers to seamlessly move and roam from place to place, city to city, and region to region with the expectation that wireless communications will continue to work transparently and reliably. Threat impacts may be described as follows:

1. Location Registers – disruption to mobility and roaming
2. Identity & Authentication Registers – disruption to security [59]
3. Mobile Switching & Packet Core Entities – disruption to network availability
4. Mobility Management Core Entity – disruption to mobility and roaming
5. Core Signaling Entities – disruption to network availability and services
6. Core Policy Entities – disruption to services

ii. Services
1. WPS – Disruption to government entities that rely upon the DHS program at the Federal, State, Local and Tribal areas relative to emergency preparedness. In the case of a mobile device connection to a landline device relying on GETS, disruption to GETS users may occur.
2. E911/NG911 – Disruption of the link to the 911 Service Provider provisioning to local PSAP ability to link emergency callers with public resources to respond to an emergency.
3. WEA – Disruption to the national mobile messaging alert system during emergencies and imminent threats.

f. Relevant Subcategories
With the exception of those subcategories identified as "out-of-Scope" the balance of the subcategories may be relevant and applicable to the generic use case, with particular emphasis on the Top Priority Subcategories (see Subcategory Priority Analysis in Section VI). In conforming to the NIST Framework, individual organizations identify their core mission(s), critical infrastructure and risks to the communications sector

[59] In addition to security, disruption may also impact network availability in the event that failure to authenticate results in network access denial, the exception being emergency services, e.g. 911.

based on aspects most relevant to ensuring the reliability and integrity of the communications infrastructure; thereby allowing for the flexibility for individual companies to self-determine how to apply the Framework.

Based on the generic use case described above and the defined top priority subcategories and risk based processes, an illustrative Generic Profile is shown below with the corresponding outcomes associated with each subcategory. The Generic Profile serves as an example, where individual organizations may choose to incorporate additional subcategories based on their individual circumstances and requirements. The corresponding outcomes illustrate how a wireless organization may apply the chosen subcategories most relevant to their business model and shows the results or outcomes to expect from having done so.

GENERIC PROFILE EXAMPLE:

Framework Categories & Subcategories (based on Top Priority Subcategories)	Corresponding Outcomes
ID.AM-1: Physical devices and systems within the organization are inventoried	Inventory of physical devices (Critical Assets) as described in Section VI
ID.AM-2: Software platforms and applications within the organization are inventoried	Inventory of software platforms and applications that correspond to Section VI
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	Assets in Section VI 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
ID.RA-1: Asset vulnerabilities are identified and documented	Vulnerabilities are assessed and regularly monitored
PR.AC-1: Identities and credentials are managed for authorized devices and users	Access control regime is implemented and audited
PR.AC-2:Physical access to assets is managed and protected	Physical access to assets defined in Section VI are managed and protected
PR.AC-3:Remote access is managed	Remote access to assets defined in Section VI is managed and resources identified to do so
PR.AC-4:Access permissions are managed, incorporating the principles of	Access control and corresponding permissions is defined and reflects

Framework Categories & Subcategories (based on Top Priority Subcategories)	Corresponding Outcomes
least privilege and separation of duties	principle of least privilege and separation of duties
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	Network is appropriately segregated as it relates to the assets identified in Section VI
PR.DS-4: Adequate capacity to ensure availability is maintained	Network capacity is monitored and maintained.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans are defined and resources identified responsible for their implementation.
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	Remote access to the assets identified in Section VI monitors and prevents unauthorized access.
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Remote access to the assets identified in Section VI implements principle of least functionality.
PR.PT-4: Communications and control networks are protected	Protection scheme implemented to cover communications and control.
DE.CM-1: The network is monitored to detect potential cybersecurity events	Cybersecurity monitoring and scans are routinely conducted.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	The physical environment for the assets in Section VI are monitored for cybersecurity threats.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	Personnel are monitored in relation to the assets in Section VI.
DE.CM-4: Malicious code is detected	Tools are implemented to look for and detect potential malicious code relative to the assets in Section VI.
RS.RP-1: Response plan is executed during or after an event	Definition of response plan and periodic “drills” are conducted.
RS.MN-1: Incidents are contained	Incident containment plan and procedure is defined, and resources identified for implementation.
RS.MN-2: Incidents are mitigated	Mitigations plans are defined and resources identified for implementation.
RC.RP-1: Recovery plan is executed during or after an event	Recovery plan is defined and resources identified for execution during and after an event.

Based on the preceding analysis of priority subcategories, risk based processes and generic use case definition the generic profile illustrates the corresponding set of outcomes. The outcomes may be achieved within the existing wireless regulatory framework to address conformity to the NIST Framework. This process is an illustrative guide to help wireless organizations consider how to apply the NIST Framework to meet the needs of their particular situation and risk model in a flexible fashion.

VIII. Conclusions & Recommendations: Wireless Segment

Based on the process and analysis outlined in Section VI above, the Wireless Segment concludes that the analysis and generic use case reflects alignment with the NIST Framework based on the defined methodology and risk assessment process. In addition the wireless segment recommends the following for consideration:

1. No new regulations are warranted in order to address conformity with the NIST Framework for the wireless segment.
2. Given the diversity within the wireless segment, continued flexibility is essential to use and conform to the NIST Framework.
3. Continued focus on Cybersecurity by NIST and CSRIC in order to avoid fragmentation of resources and efforts with regard to the diversity of government agencies that may affect wireless related cybersecurity.
4. DHS should continue to be the Sector Specific Agency for Telecom, which will further enable the advancement of the established programs and evolution of the NIST Framework. The FCC should continue to partner with industry via the Government Coordinating Council (GCC) and/or via voluntary measures such as CSRIC.
5. Consideration should be given regarding whether CSRIC IV work efforts will need to be continued during CSRIC V study and adapt to the changing threat landscape and continued alignment with the NIST Framework.
6. The wireless segment recommends that the orderly use and protection of licensed spectrum be studied in a future CSRIC in the context of the NIST Framework and Critical Infrastructure[60].
7. **Challenges to Overcome**

   As it relates to challenges to be overcome, the wireless segment defers to the conclusions defined in this report by the Barriers Feeder Group, and adds the following wireless specific items:

   - 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.
   - The diversity of technology (i.e. 2G, 3G, 4G and Wi-Fi) 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

[60] The study item would look to address the potential for moc/cloned infrastructure in licensed spectrum operating outside lawfully authorized applications, as well as how to study resources that support critical services (e.g. WPS, E911).

- The wireless ecosystem is highly diversified across original equipment manufacturers (OEMs), platform providers, operating system providers, service providers and over-the-top providers.

IX. Acknowledgments

The Wireless Segment acknowledges significant assistance and input from the Segment and Feeder Sub-groups within Working Group 4 per the list below.

1. Wireline
2. Broadcast
3. Ecosystem
4. Barriers
5. SMB
6. Cable
7. Satellite
8. Threats
9. Measurement and Metrics

X. Appendix

Informative References – limited to Assets and Services in Section VI above:

1. ISO 27001- http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
2. SANS Top 20 - http://www.sans.org/critical-security-controls/
3. X.805 - http://www.itu.int/ITU-T/worksem/ngn/200505/presentations/s5-zelstan.pdf
4. CSRIC 2A - http://transition.fcc.gov/pshs/advisory/csric/

9.5 WIRELINE SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY

The Wireline Segment group applied the NIST cybersecurity framework by developing a sample profile of prioritized recommended practices to protect wireline critical infrastructure. The approach taken by the Wireline Segment group was to develop a sample profile based upon NIST's proposed steps for the use of the NIST cybersecurity framework which include, among others, prioritizing an organizations core business/mission or objective, conducting a risk assessment to that core mission and creating a target or desired profile or state of readiness to address cyber threats.

The segment group proceeded by defining critical areas of focus or assets in scope for this analysis by applying the results from the National Sector Risk Assessment for Communications (NSRA) conducted by the Communications Sector Coordinating Council jointly with DHS in 2012. The NSRA assessed the risk to the communications infrastructure from both physical incidents and cyber-attacks. The results of this analysis concluded that while all wireline network components are vulnerable to single incidents, the risks are limited to local—and not regional or national— disruptions and/or outages. The main risk area was determined to be third party support providers, submarine cable landing sites, long haul fiber optic cables, and core transport nodes that are vulnerable to malicious actors committing resource exhaustion…a threat that poses a substantial risk to national disruptions and/or outages."

Based upon the NSRA and analysis conducted by the Segment Group, the group decided to focus the wireline critical infrastructure use case on the wireline network core infrastructure as outlined in Figure 2-3 below, and in particular core transport nodes (MPLS/TDM switching, core routing) along with submarine cable landing sites, DNS servers, and E911 routing systems and databases, which, if disrupted, would have the greatest impact on service availability on a national or regional basis consistent with the catastrophic standard for critical infrastructure discussed in Executive Order 13636.

To develop the priority practices to protect this infrastructure, the Segment Group then analyzed each of the NIST Framework's functional areas, categories and subcategories and assessed them on a variety of factors including whether each functional area, category and sub-category is in or out of scope for the infrastructure assets identified above; how they may be applied; their criticality to protecting against cyber threats (considering input from the Threats Feeder Group); and difficulty to implement (considering input from the Barriers Feeder Group including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers). The results of this analysis were used to categorize the various functional areas, categories and sub-categories and develop a list of the highest priority practices that could serve as a target profile for wireline network service providers to manage cyber risk for wireline critical infrastructure.

II. INTRODUCTION

The Wireline Segment is a subgroup within CSRIC Working Group 4 focused on reducing cybersecurity risk to wireline network infrastructure through the application of the NIST Cybersecurity Framework. The Wireline Segment evaluated CSRIC's existing cybersecurity best practices to determine how best to address alignment with the NIST Cybersecurity Framework.

III. WIRELINE SEGMENT GROUP MEMBERS

Rick Krock	Alcatel-Lucent
Chris Boyer	AT&T
Paul Diamond	Centurylink
Stacy Hartman	
Kevin Kastor	Consolidated
Dan Cashman	Fairpoint
Beau Monday	Hawaiian Telecom
Chuck Brownawell	Sprint
Robert Mayer	USTelecom
Nneka Chiazor	Verizon
Danna Valsecchi	
Greg Lucak	Windstream

Note: The wireline working group materials were also shared and feedback accepted from a variety of other segment groups including both wireline and cable.

IV. OBJECTIVE, SCOPE AND METHODOLOGY

The foundational objectives of Working Group 4 include the following[61]:

- To conform the NIST Framework to the communications sector. Identify core mission(s), critical infrastructure and risks to the communications sector and organize the NIST core Framework based on the aspects most relevant to ensuring the reliability and integrity of the core communications infrastructure.

- Maintain flexibility for individual companies. As part of this exercise, based on updated threat information and consistent with the NIST Framework, the conformed communications sector Framework will allow flexibility for individual companies to self-determine how to apply the Framework to their business based upon their individual risk profile, risk tolerance, and critical infrastructure ownership.

[61] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management Best Practices (WG4)* (2014), *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-4_Report_061814.pdf.

- Develop new streamlined practices that align with the Framework's organization and common risk management approaches. Use existing CSRIC Best Practices and other resources to inform and organize the Framework with the goal of providing companies with a "guide" of communication segment specific practices that companies may elect to implement to mitigate cyber risk.

- Develop use cases/examples of how the Framework is being used within the sector. Develop an appendix with illustrative examples or use cases about how the Framework is being used or incorporated into risk management processes of communications companies. Descriptions will be anonymized and provide examples that could be considered by all sectors regarding how aspects of the Framework could be voluntarily used.

- Provide guidance to incorporate the Framework into existing company risk management processes. Determine high level processes that companies could perform, to the extent they use the Framework, to incorporate it into their existing risk management program, or build a cyber-risk management program where none exists today.

The NIST Framework suggests seven steps for applying the Framework and, consistent with the FCC's charter for Working Group #4, allows for the Framework to be tailored by individual companies to suit their unique needs characteristics, and risks. The steps include the following:

- **Step 1: Prioritize and Scope**. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

- **Step 2: Orient**. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

- **Step 3: Create a Current Profile**. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

- **Step 4: Conduct a Risk Assessment**. This assessment could be guided by the organization's overall risk management process or previous risk assessment

activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

- **Step 5: Create a Target Profile**. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

- **Step 6: Determine, Analyze, and Prioritize Gaps**. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

- **Step 7: Implement Action Plan**. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

In order to inform wireline service providers about how to apply the Framework, the wireline segment group has applied this methodology to identify the objective, core assets, risks and prioritized common practices to develop a target profile for wireline critical infrastructure. The purpose of this profile or use case is to provide an example of the types of prioritized practices that an entity in the communications sector that owns or operates critical infrastructure may want to apply, based upon their core mission and risks, to protect that infrastructure. Individual companies should go through these steps for to develop their own cyber risk management programs.

The example use case could also be informative beyond critical infrastructure, in that the segment group would anticipate that the prioritized practices included in this example would also equally apply to other large service providers. This report serves as a guideline that wireline segment members may utilize to apply the Framework to critical infrastructure and serves as a model for how individual companies may follow a

similar process as they deem appropriate. However, it is not intended to be a checklist of standards that all organizations should follow.

In order to prioritize the NIST Framework best practices, the wireline segment collaborated with other segment teams (e.g. wireless) to review and provide input on a standard worksheet which considered the best practices according to a variety of factors. These factors included considering whether each functional area, category and sub-category were in or out of scope, how they may be applied, their criticality to protecting against cyber threats, and difficulty to implement. The working group also considered several barriers to entry including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers in assessing the degree of difficulty to implementing individual practices.

Finally, as part of the criticality assessment, the wireline segment considered the various threats that were outlined by the Threats Feeder Group. This analysis enabled the team to categorize the various functional areas, categories and sub-categories into three buckets of practices: highest priority, mid-tier and tertiary priority (as outlined in Section IV below).

V. RESULTS AND FINDINGS: WIRELINE SEGMENT

In order to create a sample profile, the wireless segment first reviewed the NIST Framework in the context of critical infrastructure. The Framework could also be viewed for other factors beyond critical infrastructure consistent with each individual sector or company's priorities and core mission applying the seven steps outlined by NIST (discussed above).

In developing a representative profile for critical infrastructure the segment considered critical infrastructure consistent with the definition discussed in President Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity[62]" which states that critical infrastructure includes those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Further, in 2012 the Communications Sector, in partnership with DHS, completed the 2012 Risk Assessment for Communications (referred to going forward as the National Sector Risk Assessment or NSRA), updating its 2008 report ,which assessed physical and cyber threats to the communications infrastructure. The risk assessment was intended to further the goals of the Communications Sector Specific Plan, also developed jointly with DHS in 2010, to identify and protect national critical network components, ensure overall network reliability, maintain "always-on" service for critical customers and quickly restore critical

[62] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013) [hereinafter *EO 13636*].

communications functions and services following a disruption. The wireline segment agreed that the scope of the efforts in working group #4 should build upon the work already completed in the 2012 risk assessment.

A. AREAS OF CRITICAL FOCUS OR ASSETS IN SCOPE

The NSRA proposes an architectural model that divides the communications network infrastructure into three components (1) services and applications, (2) core network and (3) access networks. The access portion of the wireline network is defined "as the portion that connects customers to service providers" stating that "typically, this portion of the network begins at a service provider's serving office and terminates at a customer's location, using a copper, fiber, or copper/fiber cable as the transmission medium" and that "this portion of the line may be aerial or underground, or both".

The wireline network is defined as being "composed of long haul transport networks; metro fiber rings; Fiber-to-the-Premise (FTTP); Fiber-to-the-Home (FTTH); and Fiber-to-the-x (FTTx), where x represents all potential node varieties; as well as access networks that carry voice, video, and Internet to end users. These various wireline networks remain the backbone of the communications infrastructure." The NSRA also combines the key communications features and services of the core networks into what is referred to as the "core network" and then identifies several service and application platforms such as voice, video and data.

Figure 2-2 from the 2012 risk assessment illustrates the NSRA architectural model:

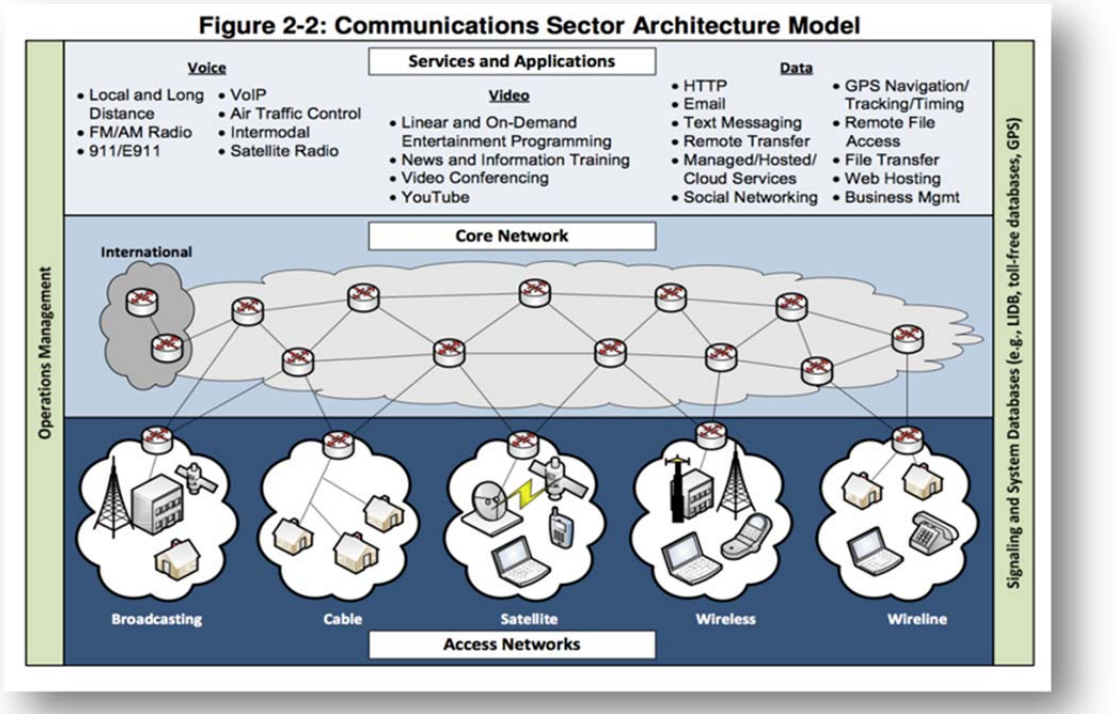
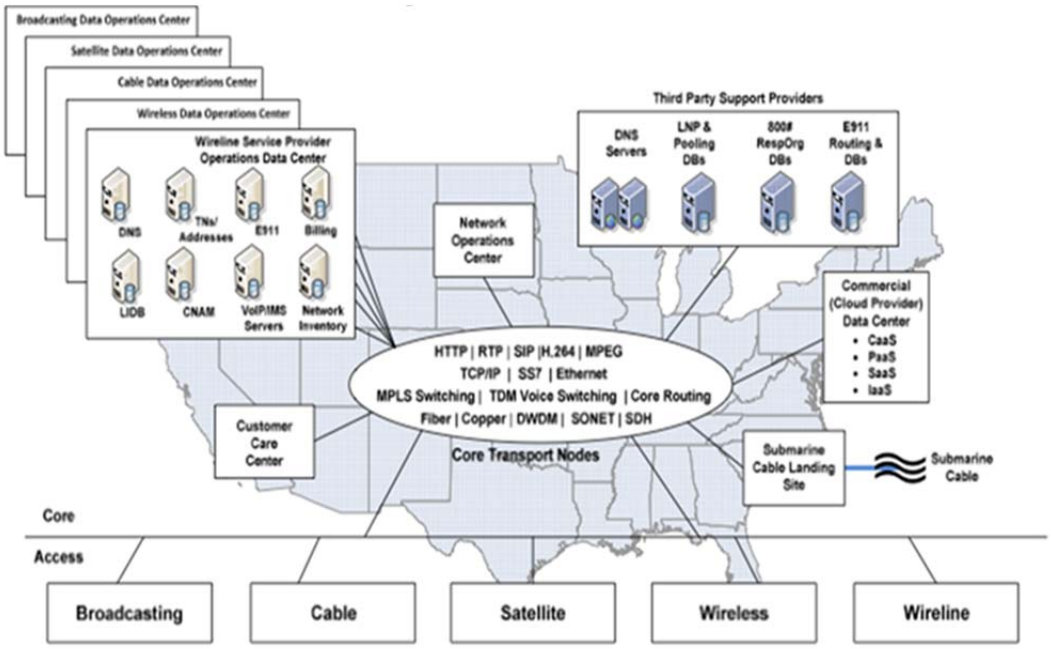


Figure 2-3 illustrates the various network components that comprise the "core network":



B. CRITICAL ASSETS/RISK MANAGEMENT

The NSRA assessed the risk to the communications infrastructure from both physical incidents and cyber-attacks. The results of this analysis concluded that while all wireline network components are vulnerable to single incidents, the risks are limited to local—and not regional or national— disruptions and/or outages. The main risk area was determined to be third party support providers, submarine cable landing sites, long haul fiber optic cables, and core transport nodes that are vulnerable to malicious actors committing resource exhaustion…a threat that poses a substantial risk to national disruptions and/or outages."

Based upon the NSRA and the analysis performed by the wireline segment group, the group decided to focus the wireline critical infrastructure use case on the wireline network core infrastructure as outlined in Figure 2-3, and in particular focusing on the core transport nodes (MPLS/TDM switching, core routing) along with submarine cable landing sites, DNS servers, and E911 routing systems and databases, which, if disrupted, would have the greatest impact on **service availability** on a national or regional basis.[63]

The wireline segment group excluded the access networks and other components of the wireline network infrastructure because, while these elements may have some exposure to cyber threats, any incident would largely be locally or regionally focused. Further, while the Domain Name System (DNS) may be in scope, the issues presented by DNS also include other parties in the ecosystem. Thus, while the Wireline Segment group can provide some DNS practices specific to wireline service providers, this topic was viewed to be out of scope for this group. With that said, there was general consensus that the government as a whole should consider addressing the broader ecosystem challenges for DNS and routing security.

C. CRITICAL SERVICES

The wireline segment focused primarily on ensuring the reliability and integrity of wireline core infrastructure which is supporting infrastructure for a wide variety of communications services including voice (both TDM voice and VoIP) and data services. In addition, the wireline segment reviewed the Framework in relation to how practices could also be applied to ensure mission critical emergency communications services such as 911 or E911.

D. ALIGNMENT WITH THE NIST CYBERSECURITY FRAMEWORK

In order to develop a target profile the wireline segment developed a prioritized set of common practices that may be applied by a wireline service provider to protect wireline

[63] It is important to note that the wireline segment group is not suggesting that the wireline network core should be considered critical infrastructure under the President's Executive Order, which designates that the Department of Homeland Security will make that determination.

critical infrastructure. The wireline segment group analyzed each of the NIST Framework's functional areas, categories and subcategories and assessed them on a variety of factors including whether each functional area, category and sub-category is in or out of scope for the infrastructure assets identified above; how they may be applied; their criticality to protecting against cyber threats (considering input from the Threats Feeder Group); and difficulty to implement (considering input from the Barriers Feeder Group including technological barriers, scale barriers, consumer/market barriers, operational barriers, and legal/policy barriers). The results of this analysis were used to categorize the various functional areas, categories and sub-categories and develop a list of the highest priority practices that could serve as a target profile for wireline network service providers to manage cyber risk for wireline critical infrastructure.

Appendix A illustrates the application methodology and results of the prioritization exercise.

1) PRIORITY PRACTICES

The following table represents the highest priority practices identified by the segment group based upon the methodology discussed above. As illustrated in Diagram XX, in applying the methodology, additional practices were considered as part of this analysis and were grouped into different categories. However, the 25 practices identified were deemed to be the priority for wireline sector members to consider implementing to provide a baseline for critical infrastructure protection. As appropriate, individual businesses can apply the methodology outlined in this report, along with the process proposed by NIST (evaluating their core business objectives/mission, risks and security needs) to determine whether to apply these and additional NIST Framework components to their critical infrastructure and/or other security needs.

HIGHEST PRIORITY PRACTICES

ID.AM-1: Physical devices and systems within the organization are inventoried	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
ID.AM-2: Software platforms and applications within the organization are inventoried	PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality
ID.GV-1: Organizational information security policy is established	PR.PT-4: Communications and control networks are protected
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	DE.CM-1: The network is monitored to detect potential cybersecurity events
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

ID.RA-1: Asset vulnerabilities are identified and documented	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats
PR.AC-1: Identities and credentials are managed for authorized devices and users	DE.CM-4: Malicious code is detected
PR.AC-2:Physical access to assets is managed and protected	RS.RP-1: Response plan is executed during or after an event
PR.AC-3:Remote access is managed	RS.MN-1: Incidents are contained
PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties	RS.MN-2: Incidents are mitigated
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	RC.RP-1: Recovery plan is executed during or after an event
PR.DS-4: Adequate capacity to ensure availability is maintained	

2) MAPPING TO CSRIC BEST PRACTICES

The segment group also considered how these prioritized practices map to the existing FCC CSRIC cybersecurity best practices. Currently there are 437 cybersecurity practices listed on the FCC's website based upon input from previous CSRIC working groups. The following is a mapping that demonstrates how some of the existing practices would apply to the prioritized practices identified in the NIST Framework.

The wireline segment group is listing these mappings solely to serve as examples that provide additional detail of steps a firm could take should they apply the priority practices identified in 6.4.1 to mitigate their cybersecurity risk. This is not a full list and is not intended to imply that wireline network service providers should apply the entire set or portions thereof. Rather, this is an example showing how some CSRIC best practices may align with the prioritized NIST practices to aid firms in determining steps they may want to consider with implementing their voluntary program. The results of this analysis are contained in Appendix B to this document.

VI. Wireline Critical Infrastructure Use Case

A. Definitions and Assumptions:

As defined in Presidential Executive Order 13636, Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The definition is taken from section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195 (c)(e)). Also for the use case below the assumption is for a large sized organization.

B. Critical Systems & Assets

As noted above in Section V, based upon the NSRA and the analysis performed by the wireline segment group, the wireline segment group focused on core transport nodes (MPLS/TDM switching, core routing) along with submarine cable landing sites, DNS servers, and E911 routing systems and databases, which, if disrupted, would have the greatest impact on service availability on a national or regional basis and critical services such as 911 or E911.

C. Threats

The segment group considered the threats inputs from the Threats Feeder Group in developing this analysis, as well as the criticality assessment outlined in the prioritization exercise in Section V.

D. Generic Profile

The following is a generic profile or use case that a company may implement to protect wireline critical infrastructure. If the prioritized practices are implemented by a company, they may have the results captured in the table below. This table is illustrative only and results will vary by company.

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 V 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

Prioritized Practice	Anticipated Outcome
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
ID.RA-1: Asset vulnerabilities are identified and documented	Vulnerabilities are assessed and regularly monitored
PR.AC-1: Identities and credentials are managed for authorized devices and users	Access control regime is implemented and audited
PR.AC-2:Physical access to assets is managed and protected	Physical access to assets defined in Section V are managed and protected
PR.AC-3:Remote access is managed	Remote access to assets defined in Section V is managed and resources identified to do so
PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties	Access control and corresponding permissions are defined and reflect principles of least privilege and separation of duties
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	Network is appropriately segregated as it relates to the assets identified in Section V
PR.DS-4: Adequate capacity to ensure availability is maintained	Network capacity is monitored and maintained
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Response plans are defined and resources responsible for their implementation are identified
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	Remote access to the assets identified in Section V are implemented to monitor and prevent unauthorized access
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Remote access to the assets identified in Section V is implemented to ensure principle of least functionality.

Prioritized Practice	Anticipated Outcome
PR.PT-4: Communications and control networks are protected	Protection scheme implemented to cover communications and control
DE.CM-1: The network is monitored to detect potential cybersecurity events	Cybersecurity monitoring and scans are routinely conducted
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	The physical environment for the assets in Section V are monitored for cybersecurity threats
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	Personnel are monitored in relation to the assets in Section V
DE.CM-4: Malicious code is detected	Tools are implemented to look for and detect potential malicious code relative to the assets in Section V
RS.RP-1: Response plan is executed during or after an event	Definition of response plan and periodic "drills" are conducted
RS.MN-1: Incidents are contained	Incident containment plan and procedure are defined and resources identified for implementation
RS.MN-2: Incidents are mitigated	Mitigations plans are defined and resources identified for implementation.
RC.RP-1: Recovery plan is executed during or after an event	Recovery plan is defined and resources identified for execution during and after an event

VII. Conclusions and Recommendations

- Given the diversity within the wireline segment, continued flexibility is essential to use and conform to the NIST Framework. Wireline network operators are best positioned to understand their cybersecurity risks and should be afforded flexibility to apply the Framework to their business needs.

- The FCC should continue to partner with industry to promote the voluntary use of the NIST Cybersecurity Framework 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 continue to collaborate with NIST and DHS in the further development of the NIST Cybersecurity Framework and promote programs to increase the voluntary use of the CSF.

- The FCC should partner with other departments and agencies to promote education and awareness of the cybersecurity risks inherent in critical communications infrastructures, and promote steps that the communications sector can take to provide external stakeholders with macro-level assurance that collective actions are reducing cybersecurity risks.

- The FCC should continue to provide flexibility to organizations and base use of the framework based upon risk management principles of identifying critical assets, risks and developing mitigation plans accordingly.

CSRIC Working Group 4
Wireline Segment Report
Appendix A

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

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
ID.BE-1: Organization's role in the supply chain is identified and communicated	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated	In Scope	Critical infrastructure or as part of cyber risk management program.	3	5
ID.BE-3: Priorities for organizational mission, objectives and actives are established and communicated	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	In Scope	Critical infrastructure or as part of cyber risk management program.	3	5
ID.BE-5: Resilience requirements to support delivery of critical services are established	In Scope	Critical infrastructure or as part of cyber risk management program.	3	5
ID.GV-1: Organizational information security policy is established	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3
ID.GV-4: Governance and risk management processes address cybersecurity risks	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
ID.RA-1: Asset vulnerabilities are identified and documented	Rephrase - Asset vulnerabilities and threats are identified	Critical infrastructure or as part of cyber risk management program.	5	4
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	In Scope	Critical infrastructure or as part of cyber risk management program.	2	5
ID.RA-3: Threats, both internal and external, are identified and documented	Rephrase - Asset vulnerabilities and threats are documented	Critical infrastructure or as part of cyber risk management program.	1	4
ID.RA-4: Potential business impacts and likelihoods are identified	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	In Scope	Critical infrastructure or as part of cyber risk management program.	4	4
ID.RA-6: Risk responses are identified and prioritized	In Scope	Critical infrastructure or as part of cyber risk management program.	4	4

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	In Scope	Critical infrastructure or as part of cyber risk management program.	3	4
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	In Scope - only for personnel that work with critical infrastructure assets	Critical infrastructure or as part of cyber risk management program.	1	3
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	In Scope - same as above	Critical infrastructure or as part of cyber risk management program.	1	5
PR.AC-1: Identities and credentials are managed for authorized devices and users	In Scope	Critical infrastructure or as part of cyber risk management program.	5	4
PR.AC-2:Physical access to assets is managed and protected	In Scope	Critical infrastructure or as part of cyber risk management program.	5	4
PR.AC-3:Remote access is managed	In Scope	Critical infrastructure or as part of cyber risk management program.	5	4
PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties	In Scope	Critical infrastructure or as part of cyber risk management program.	5	4
PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate	In Scope	Critical infrastructure or as part of cyber risk management program.	5	4

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
PR.AT-1: All users are informed and trained	In Scope	Critical infrastructure or as part of cyber risk management program.	2	4
PR.AT-2: Privileged users understand roles & responsibilities	In Scope	Critical infrastructure or as part of cyber risk management program.	3	5
PR.AT-3: Third-party stakeholders (e.g., suppliers customers, partners) understand roles & responsibilities	In Scope	Critical infrastructure or as part of cyber risk management program.	3	5
PR.AT-4: Senior executives understand roles & responsibilities	Only senior executives that are responsible for overseeing critical infrastructure	Critical infrastructure or as part of cyber risk management program.	3	5
PR.AT-5: Physical and information security personnel understand roles and responsibility	Only information security personnel that are responsible for overseeing critical infrastructure	Critical infrastructure or as part of cyber risk management program.	4	5
PR.DS-1: Data-at-rest is protected	In Scope	Critical infrastructure or as part of cyber risk management program.	4	4
PR.DS-2: Data-in-transit is protected	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.DS-3: Assets are formally managed throughout removal, transfers and disposition	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.DS-4: Adequate capacity to ensure availability is maintained	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
PR.DS-5: Protections against data leaks are implemented	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	In Scope	Critical infrastructure or as part of cyber risk management program.	4	2
PR.DS-7: The development and testing environment(s) are separate from the production environment	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	In Scope	Critical infrastructure or as part of cyber risk management program.	2	2
PR.IP-2: A System Development Life Cycle to manage systems is implemented	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
PR.IP-3: Configuration change control processes are in place	In Scope	Critical infrastructure or as part of cyber risk management program.	3	3
PR.IP-4: Backups of information are conducted, maintained and tested periodically	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	In Scope	Critical infrastructure or as part of cyber risk management program.	2	4

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
PR.IP-6: Data is destroyed according to policy	In Scope	Critical infrastructure or as part of cyber risk management program.	3	3
PR.IP-7: Protection processes are continuously improved	In Scope	Critical infrastructure or as part of cyber risk management program.	3	3
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	In Scope	Critical infrastructure or as part of cyber risk management program.	1	5
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
PR.IP-10: Response and recovery plans are tested	In Scope	Critical infrastructure or as part of cyber risk management program.	3	2
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
PR.IP-12: A vulnerability management plan is developed and implemented	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
PR.MA-2: Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	In Scope	Critical infrastructure or as part of cyber risk management program.	3	3
PR.PT-2: Removable media is protected and its use restricted according to policy	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
PR.PT-4: Communications and control networks are protected	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
DE.AE-2: Detected events are analyzed to understand attack targets and methods	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	In Scope	Critical infrastructure or as part of cyber risk management program.	4	1

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
DE.AE-4: Impact of events is determined	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
DE.AE-5: Incident alert thresholds are established	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
DE.CM-1: The network is monitored to detect potential cybersecurity events	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity threats	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
DE.CM-4: Malicious code is detected	In Scope	Critical infrastructure or as part of cyber risk management program.	5	1
DE.CM-5: Unauthorized mobile code is detected	In Scope	Critical infrastructure or as part of cyber risk management program.	2	1
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	In Scope	Critical infrastructure or as part of cyber risk management program.	2	2
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	In Scope	Critical infrastructure or as part of cyber risk management program.	4	2

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
DE.CM-8: Vulnerability scans are performed	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	In Scope	Critical infrastructure or as part of cyber risk management program.	2	4
DE.DP-2: Detection activities comply with applicable requirements	In Scope	Critical infrastructure or as part of cyber risk management program.	4	2
DE.DP-3: Detection processes are tested	In Scope	Critical infrastructure or as part of cyber risk management program.	2	2
DE.DP-4: Event detection information is communicated to appropriate parties	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
DE.DP-6: Detection processes are continuously improved	In Scope	Critical infrastructure or as part of cyber risk management program.	3	2
RS.RP-1: Response plan is executed during or after an event	In Scope	Critical infrastructure or as part of cyber risk management program.	5	2
RS.CO-1: Personnel know their roles and order of operations when a response is needed	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
RS.CO-2: Events are reported consistent with established criteria	In Scope	Critical infrastructure or as part of cyber risk management program.	3	4

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
RS.CO-3: Information is shared consistent with response plans	In Scope	Critical infrastructure or as part of cyber risk management program.	3	4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Out of Scope	Critical infrastructure or as part of cyber risk management program.		
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	In Scope	Critical infrastructure or as part of cyber risk management program.	3	2
RS.AN-1: Notifications from detection systems are investigated	In Scope	Critical infrastructure or as part of cyber risk management program.	4	3
RS.AN-2: The impact of the incident is understood	In Scope	Critical infrastructure or as part of cyber risk management program.	3	3
RS.AN-3: Forensics are performed	In Scope	Critical infrastructure or as part of cyber risk management program.	2	1
RS.AN-4: Incidents are categorized consistent with plans	In Scope	Critical infrastructure or as part of cyber risk management program.	1	2
RS.MN-1: Incidents are contained	In Scope	Critical infrastructure or as part of cyber risk management program.	5	1
RS.MN-2: Incidents are mitigated	In Scope	Critical infrastructure or as part of cyber risk management program.	5	1

Sub-Category	In Scope/Out of Scope	Application	Prioritization	
			Criticality	Difficulty
RS.MN-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	In Scope	Critical infrastructure or as part of cyber risk management program.	4	2
RS.IM-1: Response plans incorporate lessons learned	In Scope	Critical infrastructure or as part of cyber risk management program.	1	4
RS.IM-2: Response strategies are updated	In Scope	Critical infrastructure or as part of cyber risk management program.	1	4
RC.RP-1: Recovery plan is executed during or after an event	In Scope	Critical infrastructure or as part of cyber risk management program.	5	3
RC.RP-1: Recovery plans incorporate lessons learned	In Scope	Critical infrastructure or as part of cyber risk management program.	1	3
RC.RP-2: Recovery strategies are updated	In Scope	Critical infrastructure or as part of cyber risk management program.	1	3

FP #	Framework Practice	Examples from CSRIC Best Practices	
ID.AM-1:	Physical devices and systems within the organization are inventoried	9-9-8037 Network Operators, Service Providers, and Public Safety should maintain a complete inventory of elements to ensure that patches/fixes can be properly applied across the organization. This inventory should be updated each time a patch/fix is identified and action is taken.	9-8-8750 Risk Assessments: Service providers and network operators should have assigned risk ratings for vulnerabilities and definitions of those risk ratings (i.e. What does a High risk vulnerability mean to the general user public? etc.) Finally the security team should have access to an accurate and readily available asset inventory (See Step 1: Asset Inventory) (including the asset owners, and patch levels) and network diagrams.
PR.IP-9:	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	9-8-8549 Lack of Business Recovery Plan: When a Business Recovery Plan (BRP) does not exist; Service Providers and Network Operators should bring together an ad-hoc team to address the current incident. The team should have technical, operations, legal, and public relations representation. Team should be sponsored by senior management and have a direct communication path back to management sponsor. If situation exceeds internal capabilities consider contracting response/recovery options to 3rd party security provider.	9-9-8068 Service Providers, Network Operators, Public Safety, and Equipment Suppliers should develop and practice a communications plan as part of the broader Incident response plan identifying key players to include as many of the following items as appropriate: contact names, business telephone numbers, home telephone numbers, pager numbers, fax numbers, cell phone numbers, home addresses, internet addresses, permanent bridge numbers, etc. Notification plans should be developed prior to an event/incident happening where necessary. The plan should also include alternate communications channels (e.g., alpha pagers, internet, satellite phones, VOIP, private lines, smart phones) balancing the value of any alternate method against the security and information loss risks introduced.

FP #	Framework Practice	Examples from CSRIC Best Practices	
ID.AM-2:	Software platforms and applications within the organization are inventoried	9-9-8037 Network Operators, Service Providers, and Public Safety should maintain a complete inventory of elements to ensure that patches/fixes can be properly applied across the organization. This inventory should be updated each time a patch/fix is identified and action is taken.	9-8-8750 Risk Assessments: Service providers and network operators should have assigned risk ratings for vulnerabilities and definitions of those risk ratings (i.e. What does a High risk vulnerability mean to the general user public? etc.) Finally the security team should have access to an accurate and readily available asset inventory (See Step 1: Asset Inventory) (including the asset owners, and patch levels) and network diagrams.
PR.MA-2:	Remote maintenance of organizational assets is performed in a manner that prevents unauthorized access	9-6-5165 Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers (e.g., remote software developers) have the equipment and support necessary to secure their computing platforms and systems to the equivalent level of those on-site. Security software, firewalls and locked file cabinets are all considerations.	9-8-0785 Network Operation Center (NOC) Communications Remote Access: Network Operators and Service Providers should consider secured remote access to critical network management systems for network management personnel working from distributed locations (e.g., back-up facility, home) in the event of a situation where the NOC cannot be staffed (e.g., pandemic).
ID.AM-5:	Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	9-7-5022 Network Operators, Service Providers and Equipment Suppliers should internally identify and document areas of critical infrastructure as part of security and emergency response planning. This documentation should be kept current and protected as highly sensitive proprietary information.	
PR.PT-3:	Access to systems and assets is controlled, incorporating the principle of least functionality	9-9-8086 Network Operators, Service Providers, Public Safety, and Equipment Suppliers based on the principles of least–privilege (the minimum access needed to perform the job) and separation of duties (certain users perform certain tasks) should develop capabilities and processes to determine which users require access to a specific device or application.	
ID.GV-1:	Organizational information security policy is established		

FP #	Framework Practice	Examples from CSRIC Best Practices	
PR.PT-4:	Communications and control networks are protected	9-8-8015 Segmenting Management Domains: For OAM&P activities and operations centers, Service Providers and Network Operators should segment administrative domains with devices such as firewalls that have restrictive rules for traffic in both directions and that require authentication for traversal. In particular, segment OAM&P networks from the Network Operator's or Service Provider's intranet and the Internet. Treat each domain as hostile to all other domains. Follow industry recommended firewall policies for protecting critical internal assets.	
ID.GV-2:	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	9-7-5031 Network Operators, Service Providers and Equipment Suppliers should establish a role for the security function (i.e., physical and cyber) in business continuity planning, including emergency response plans and periodic tests of such plans.	
DE.CM-1:	The network is monitored to detect potential cybersecurity events	9-9-0401 Network Operators, Service Providers, and Public Safety should monitor their network to enable quick response to network issues.	
ID.GV-3:	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed		9-8-8922 Privacy Considerations in Botnet Detection, Notification, and Remediation: Because technical measures to (a) detect compromised end-user devices, (b) notify end-users of the security issue, and (c) assist in addressing the security issue, may result in the collection of customer information (including possibly personally identifiable information and other sensitive information, as well as the content of customer communications), ISPs should ensure that all such technical measures address customers privacy, and comply and be consistent with all applicable laws and corporate privacy policies.

FP #	Framework Practice	Examples from CSRIC Best Practices	
DE.CM-2:	The physical environment is monitored to detect potential cybersecurity events		
ID.RA-1:	Asset vulnerabilities are identified and documented	9-9-8071 Threat Awareness: Service providers and Network Operators should subscribe to vendor patch/security notifications and services to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network.	
DE.CM-3:	Personnel activity is monitored to detect potential cybersecurity threats		
PR.AC-1:	Identities and credentials are managed for authorized devices and users	9-8-8601 Wi-Fi Policies: Service Providers and Network Operators should establish policies to ensure only authorized wireless devices approved by the network managing body or network security are allowed on the network. Unauthorized devices should be strictly forbidden.	
DE.CM-4:	Malicious code is detected	9-7-0542 Equipment Supplier processes (e.g., software upgrade) should include prevention and detection of malicious code insertion from Original Equipment Manufacturers (OEMs), contractors, and disgruntled employees.	9-7-5218 Equipment Suppliers should implement a comprehensive security program for protecting hardware, firmware and software from malicious code insertion or tampering during development and delivery, taking into consideration that some developmental environments around the world present a higher risk level than others.
PR.AC-2:	62 best practices Physical access to assets is managed and protected	9-7-5010 Network Operators, Service Providers and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.	

FP #	Framework Practice	Examples from CSRIC Best Practices	
RS.RP-1:	Response plan is executed during or after an event	9-7-0779 Network Operators, Service Providers and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	9-7-5031 Network Operators, Service Providers and Equipment Suppliers should establish a role for the security function (i.e., physical and cyber) in business continuity planning, including emergency response plans and periodic tests of such plans.
PR.AC-3:	Remote access is managed	9-6-5165 Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers (e.g., remote software developers) have the equipment and support necessary to secure their computing platforms and systems to the equivalent level of those on-site. Security software, firewalls and locked file cabinets are all considerations.	
RS.MN-1:	Incidents are contained		
PR.AC-4:	Access permissions are managed, incorporating the principles of least privilege and separation of duties	9-9-8086 Network Operators, Service Providers, Public Safety, and Equipment Suppliers based on the principles of least–privilege (the minimum access needed to perform the job) and separation of duties (certain users perform certain tasks) should develop capabilities and processes to determine which users require access to a specific device or application.	
RS.MN-2:	Incidents are mitigated		
PR.AC-5:	Network integrity is protected, incorporating network segregation where appropriate	9-9-8008 Network Operators, Service Providers, and Public Safety should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks be separated and partitioned from one another.	

FP #	Framework Practice	Examples from CSRIC Best Practices	
RC.RP-1:	Recovery plan is executed during or after an event	9-7-0779 Network Operators, Service Providers and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	
PR.DS-4:	Adequate capacity to ensure availability is maintained		

9.6 REQUIREMENTS AND BARRIERS TO IMPLEMENTATION CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4 March 2015

TABLE of CONTENTS

I. Executive Summary

The Requirements and Barriers to Implementation feeder group was tasked with identifying the available protocols, resources and tools that would be necessary for organizations to deploy in order to effectuate alignment with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework ("Framework") as well as examine barriers and other challenges to communications sector organizations' implementation of the Framework. In order to identify these requirements and barriers, the feeder group conducted interviews with each segment group and conducted an in-depth analysis of the NIST Framework down to the subcategory level, to identify operational and technical requirements.

Through interviews with the Segment groups, the feeder team found that existing CSRIC-IV resources, specifically WG5 on Remediation of Server-Based DDoS Attacks, presented us with a thoughtful framework for examining implementation challenges. Building on the WG5 work, the Requirements and Barriers Feeder Group identified five primary types of barriers to Framework implementation:

1. Financial barriers
2. Legal barriers
3. Technical barriers
4. Consumer/market barriers
5. Operational barriers

Chief among these barriers are the financial costs of implementing the Framework. While for large organizations the cybersecurity practices outlined in the NIST Framework would largely be considered just a cost of doing business, the majority of small to medium-sized organizations would view these as costs with no calculable direct return on investment. The Requirements and Barriers Feeder Group suggests several methods for mitigating financial barriers to implementation including recommending the federal government continue the work on creating a menu of market incentives -- initiated by the U.S. Departments of the Treasury, Commerce, and Homeland Security, and the General Services Administration (GSA)/Department of Defense (DOD) joint effort– that was initiated in EO 13636. Other incentives the feeder group recommends include increased liability protections, Expansion of the National Wireless Initiative to include Framework Implementation Tiers**,** SAFETY Act designations, and other tax incentives.

As part of its comprehensive analysis of existing protocols and resources, the Requirements and Barriers Feeder Group analyzed the entire NIST Cybersecurity Framework down to the sub-category level to identify operational and technical requirements for all 98 sub-categories. Recognizing that people and processes are the heart of any implementation, the feeder group's broadened examination looked at requirements involving human resources, specific expertise, training, and the processes necessary for achieving the subcategory recommendation. These operational and technical requirements were ultimately incorporated into the feeder group's

findings and recommendations, as well as the comprehensive Appendix A that includes informative references.

II. Introduction

The Requirements and Barriers to Implementation feeder group was tasked with considering whether barriers exist that challenge the ability of communications companies with implementing the NIST Framework. Besides examining barriers, the feeder group sought to elicit methods by which these barriers might be overcome.

A. Feeder Group Structure

The Requirements and Barriers to Implementation working group consist of the members listed below:

Name	Company
Larry Clinton (Co-Chair)	Internet Security Alliance
Harold Salters (Co-Chair)	T-Mobile
Richard Krock	Alcatel-Lucent
Chris Garner	CenturyLink
Stacy Hartman	CenturyLink
Matthew Starr	CompTIA
Chris Smith	Consolidated Communications
Emily Talaga	FCC
Jim Capers	Hawaiian Telecom
Merike Kaeo	Internet Identity
Tanner Doucet	Internet Security Alliance
Ed Czarnecki	Monroe Electronics
Brad Ramsay	NARUC
Pam Witmer	PA PUC
Brian Scarpelli	TIA
Arthur (Trey) Jackson	T-Mobile
Tom Soroka	USTelecom Association
Heath McGinnis	Verizon

B. Background

1) Financial

Research from Pricewaterhouse[64], CIO Magazine[65], CSIS[66], and McAfee[67] has consistently found that cost is the single biggest barrier to implementing adequate cybersecurity for critical infrastructure. Historically, this has been less true for large organizations. Large enterprises have traditionally marshaled the financial and the human resources necessary to evaluate where the enterprise stands with respect to the 98 categories and subcategories of the Framework.

However, as cyber threats continue to evolve, financial considerations could become a more pressing issue - even for larger enterprises. In particular, an increase in attacks by nation states on private firms could substantially alter the economic equation with respect to cybersecurity. Any private company, regardless of their extensive use of the Framework, is unlikely to be able to withstand a concerted attack from a sophisticated nation-state that is attempting to breach its system. In addition, larger companies can be compromised through the thousands, sometimes tens of thousands, of interconnections they have with smaller players whose use of the Framework may be impractical to fully track.

Small and medium-sized businesses, however, have much more limited operating and capital resources, and require a stricter prioritization regimen that is often driven by the return on investment (ROI). With this in mind, it is important to recognize that determining the ROI for the technology and processes that underlie an organization's cybersecurity posture is very difficult and ultimately makes identifying the mix of technologies and processes to invest in difficult. Money spent on security controls which cannot be accurately analyzed to determine their value can result in more austere fiscal environments – thus creating more financial barriers to implementation. For small and medium businesses, these uncertainties can accumulate and further erode efforts to boost the enterprise's cybersecurity posture and/or maturity level.

The time and resources it may take for an organization to systematically go through all 98 categories and sub-categories of the Framework should be taken into consideration when examining financial barriers. Since it is unclear what "framework implementation" means, the time and money it takes for an organization to determine

[64] *See* PricewaterhouseCoopers ('PwC'), *Changing the Game – Key Findings from the Global State of Information Security* (2013), *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf.
[65] *See* Chief Executive Officer Magazine, http://www.cio.com/about/about.html (last visited Mar. 13, 2015).
[66] *See* Center for Strategic and International Studies, http://csis.org/ (last visited Mar. 13, 2015).
[67] *See* McAfee and the Center for Strategic and International Studies, *The Economic Impact of Cybercrime and Cyber Espionage* (2013), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

what implementation means for them (both onetime cost and continuing costs) can be considered a significant barrier to implementation.

2) **Legal**

The main legal/policy barrier to Framework implementation is the uncertainty around information sharing. There is consensus among the sub-team participants that the current lack of a legislative foundation to facilitate information sharing serves as a barrier to implementation. The sub-team believes that legislation which supports increased liability protections for information sharing would decrease uncertainty and allow for a more proactive approach to implementing better cybersecurity information sharing practices.

3) **Technology**

There is uncertainty around the value of certain technologies, which relates to the financial barriers discussed above – particularly the barrier regarding the inability to determine the ROI of implementing a single technology solution or suite of technologies. The degree to which technology can be a barrier to implementation of the NIST framework is fundamentally a function of an enterprise's resources, as further tempered by the enterprise's Tier position and their risk management profile.

4) **Consumer/Market**

Consumers, who largely do not know or care about NIST Framework implementation, generally want to trust that security is embedded in and working for the products and services they utilize. As such, the sub-team believes that NIST framework implementation, which it assumes will result in increased security, will be a market incentive. Correspondingly, while customers often care about security, notifications sent to customers that are compromised may do little to improve overall security. Additionally, consumers may be alarmed when notified about compromised security – which can result in them expressing concerns about the privacy of their data.

5) **Operational**

The lack of ability to provide quantifiable metrics to demonstrate that implementing the Framework actually increases security may serve as a barrier to future implementation. If companies are unable to identify reasonable metrics that demonstrate security is being improved through the Framework's 98 sub-categories, then companies may be less likely to implement the Framework.

While there may be a diversity of threats facing the communications sector, there are common vulnerabilities that, if properly addressed, can be leveraged to overcome barriers, which are more fully discussed below. The NIST Framework presents Informative References that can be analyzed to identify solutions to common modes of exploitation.

III. Objective, Scope and Methodology

The objective of the requirements and barriers feeder group was to assess the required resources (both operational and technical) that an entity needs to implement the NIST Framework and to identify the various barriers that entities may need to overcome to successfully implement the NIST C Framework.

In order to accomplish this work, the requirements and barriers feeder group initiated 1) an interview and analysis effort and 2) a NIST Framework requirements and barriers effort.

The interview and analysis effort/work was performed by interviewing representatives from Working Group 4's four industry segments (Wireline, Wireless, Satellite and Cable) and the Small/Medium Business Feeder Group. These interviews consisted of discussions around the 22 categories of the NIST Framework and the implementation challenges that existed. These challenges were then considered using the analytic barriers framework that was first introduced by CSRIC III Working Group 7[68] (i.e., financial, legal/policy, technological, consumer/market and operational), and also employed by CSRIC IV Working Group 5[69].

As the second part of the overall Requirements and Barriers effort, the entire NIST Cybersecurity Framework was analyzed to identify operational and technical requirements for all 98 sub-categories of the Framework. The subgroup categorized the subcategory recommendation where the requirements involved human resources, specific expertise, training, teams of people, and the processes necessary for achieving the subcategory recommendation, as "Operational Requirements". For every subcategory recommendation where the requirements involved technology resources, systems, software, tools and the associated technical functions necessary for achieving the subcategory recommendation, as the group categorized as "Technology Requirements".

All of the newly defined operational and technology requirements were then evaluated for various types of impediments that could occur when implementing the Framework. These impediments resulted in the barriers that were identified and outlined below for each of the 98 subcategories of the NIST Framework.

These operational and technical requirements, along with the corresponding identified barriers to implementing the 98 subcategories of the NIST Framework were drawn from the collective operational and technical experience of the subject matter experts participating on the Requirements and Barriers subgroup, as well as from the NIST Special Publication 800-53,

---

[68] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council III, *Working Group 5 - DNSSEC Implementation Practices for ISPs Final Report on Measurement of DNSSEC Deployment* (2013), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.pdf.

[69] *See* Federal Communications Commission, The Communications Security, Reliability and Interoperability Council IV - Working Group 5, *WORKING GROUP 5 Remediation of Server - Based DDoS Attacks Final Report* (2014), http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

Security and Privacy Controls for Federal Information Systems and Organizations, along with the documents and COBIT framework developed by the Information Systems Audit and Control Association (ISACA). The culmination of this effort resulted in a table depicting all of the NIST Framework main categories, the 98 framework subcategories, the requirements and barriers, and the specific references to the NIST Special Publication 800-53 and ISACA documents. This table can be found in the Appendix of this document[70].

A. Results and Findings

The following feedback was provided during surveys with the Wireless, Wireline, Cable and Satellite segments, as well as the Small and Medium Business Feeder Group:

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)
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**Technology:** There is no specific set of technologies for implementing the framework, as they are evolving and changing. Barrier is the complexity of the problem. Nonetheless, full assessment of the Business Environment should be undertaken as a starting point for risk management calculations. (TECHNOLOGY)
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**Legal/Policy:** Difficulties in differentiating between what is classified and what is non-classified information. For segments like Satellite, differentiation between the federal government (classified) and consumer/enterprise markets (unclassified) makes governance determinations more

[70] The exact document references are described in the right most column of the requirements and barriers table in the Appendix.

	complex. (LEGAL/POLICY)
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Operational:** Challenge in obtaining and being able to discern what information is reliable and what is not in a complex threat environment. Nonetheless, undertaking a Risk Assessment on a best-available basis is a necessary starting point for risk management calculations. (OPERATIONAL)
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**Financial:** There is little cyber empirical data to support ROI calculations, as it is very difficult to determine risk exposure. Barriers can be mitigated, however, through the use of informed risk management resources, such as the National Association of Corporate Director's Cyber Risk Oversight Handbook, published in collaboration with the Internet Security Alliance.

2) Protect Function

Relevant Categories:	**Primary Barrier:**
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**Financial:** Legacy systems require significant investments to implement framework, and there would be a lower ROI. Companies should use the NIST Tier position analysis to determine where they currently are, and where they want to be. (FINANCIAL)
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**Operational:** Difficult to implement and gauge effectiveness of training in a complex threat environment. (OPERATIONAL)

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**Financial:** Money spent on security controls cannot be accurately analyzed to determine their value. Companies should use the NIST framework's Tiers to determine where they currently are, and where they want to be. (FINANCIAL)
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**Technology:** Wide diversity of technologies and available solutions is a complexity barrier. Although unique systems, enterprises should analyze for common vulnerabilities/modes of exploitation that can be leveraged to overcome barriers. (TECHNOLOGY)
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**Operational:** Implementing the Framework does not ensure that it is being followed through as part of the business model. Enterprises should seek to align the Framework with on-going operations wherever possible. (OPERATIONAL)
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**Operational:** Usage can be monitored, but it can be very difficult to understand the effect. Using the NIST Framework Tier position analysis, organizations can prioritize security measures. (OPERATIONAL)

3) Detect Function

Relevant Categories:	Primary Barrier:
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**Operational:** Difficult to determine the impact in real-time. Enterprises should seek to align the Framework with on-going operations wherever possible. (TECHNOLOGY)

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**Operational:** Companies are not actively monitoring all employee activity. Implementing would require additional investments. Using the NIST Tier position analysis, organizations can prioritize security measures. (OPERATIONAL)
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**Financial:** There will be an additional CAPEX cost to procuring SIEM / IPS / IDS technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for SIEM / IPS / IDS technologies and systems.

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.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**Legal/Policy:** Liability concerns could limit voluntary information sharing. Liability Protection via CISPA and other Bills, as well as liability protection from self-audit, should mitigate this barrier. (LEGAL/POLICY)
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery	**Operational:** Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident

activities.	response / and specialized technologies will hinder an effective response to an attack, breach or loss of data.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**Financial:** The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack costing them time and money
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**Financial:** Numerous False alarms, lack of dedicated security staff, lack of staff availability, lack of budget all could affect the organizations ability to keep their response strategies up to date.

5) Recover Function

Relevant Categories:	**Primary Barrier:**
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**Financial:** There will be an additional CAPEX cost to procuring DR technologies and off-site services like storage and data recovery. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Business Continuity and Disaster Recovery
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**Operational:** Lack of BC/DR Plans will hinder an effective recovery from an attack, breach or loss of data.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**Operational:** Some staff, executives, shareholders and board members may disagree with the content and delivery time of press releases and official notifications.

IV. Conclusions and Recommendations

There is currently a large and growing set of independent research, which has consistently shown that the primary problem with respect to securing critical infrastructure is economic. Sources as varied as PWC, McAfee/Intel, CIO Magazine, and the Center for Strategic and International Studies (CSIS).

As a general matter, mitigating some of the costs involved with voluntary adoption of the Framework will increase awareness and overall implementation, particularly for small-to-medium enterprises. Therefore, the barriers feeder group recommends that the federal government resume the work on incentives that was initiated by four government agencies– U.S. Departments of the Treasury, Commerce, and Homeland Security, and a General Services Administration (GSA)/Department of Defense (DOD) joint effort– that was called-for in EO 13636.

Even relatively homogenous critical infrastructure sectors, such as the Communications Sector, often have substantial differences at the individual enterprise level. Incentives may need to be applied at the corporate level to be effective, and only each individual corporate entity would be in a position to evaluate what policies and incentives work best for them. Therefore, a menu of market incentives available for corporations that elect voluntary adoption of effective standards and practices would best drive further adoption of the Framework.

The barriers feeder group suggests the FCC consider, and advocate for the federal government at-large to develop a set of economic incentives that will further Framework adoption.

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 hardware resources need to be purchased and administered.	· **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

		ID.AM-2: Software platforms and applications within the organization are inventoried	**Operational Requirement(s):** Appropriate and adequate Operations staff should be assigned to locate, track, count, and document all network critical infrastructure software, critical applications, OSS software, (i.e.; Billing & Customer Account DBs), network/customer databases, mobile employee supporting systems, and stored information that is critical to the operations of the organization. * Additional levels of staff trust and training may be established for this requirement. **Technology Requirement(s):** Operations staff assigned to inventory network critical software may use easy to operate database software and technologies that can automate, scale and report on the adding and removing of network software resources that are inventoried. This automated system can detect the presence of unauthorized software, databases and applications. * It is highly recommended that software licenses, GNU-Open source software, software additions/deletions, and software version control be included in the software inventory database system. * This software inventory system should be made secure to prevent corruption of critical network functions, to prevent theft of software and to prevent fraudulent actions. * It is highly recommended that access to this software inventory is extremely limited to those with a need-to-know basis. **Barriers:** Professional staff should be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. 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 hardware resources need to be purchased and administered.	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3:	**Operational Requirement(s):**	· **CCS CSC** 1

		Organizational communication and data flows are mapped	The organization can determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization can take into account "all" internal communications with: *Tiers I,II,III of operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc.* * Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how can be documented and conveyed through ongoing training, to the effected personnel. When organizations determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. The organization can take into account "all" external communications with: *vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, , service providers, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc*. * Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how can be documented and conveyed through ongoing training, to the effected personnel. * Organizations may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. * Organization can develop a baseline security compliance policy for all external components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) Additionally the process may maintain a tracking and audit mechanism. **Technology Requirement(s):**	· **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8

			Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems can all have the *scheduling, credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. * Security policy filters can be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. * The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. **Barriers:** Mapping an organization's communications flow will require assigning and allocating staff (that may be assigned to other functions), to document this flow and to keep it updated with business and personnel changes.	
		ID.AM-4: External information systems are catalogued	**Operational Requirement(s):** Organizational staff can identify, inventory, track and update the catalog of externally facing critical infrastructure systems, databases, web servers, virtual machines, virtual/physical circuits, networks, VPNs, VLANs, WANs, communications channels, email systems, phone/UC systems, calendars, applications, web portals, eCommerce interfaces, mobile/remote employee devices, cloud-data center resources and any other hardware and software that is used to communicate with "outside" entities. Outside entities include but not limited to: *vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, executive communications, billing interfaces, eCommerce interfaces, mobile employee support, cloud-data centers etc*. * Organization can establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. * Organization can develop rules for external providers to comply with and employ measures to monitor security control compliance.	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9

			Technology Requirement(s): Organizational staff assigned to catalog externally facing critical infrastructure information systems, servers, virtual machines, software, networks and resources can use easy to operate database software and technologies that can scale and report on the externally facing resources that are inventoried. This externally facing catalog system can be made secure to prevent corruption of critical network functions, to prevent theft of services/software and to prevent fraudulent actions. It is highly recommended that access to this external system catalog is extremely limited to those with a need-to-know basis. **Barriers:** The Operational requirements to catalog externally facing critical infrastructure information systems, software, networks and resources will require assigning and allocating staff (that may be assigned to other functions), to document this catalog and to keep it updated with business and personnel changes.	
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**Operational Requirement(s):** Organizational leadership, operations and engineering staff may determine the primary-critical infrastructure functions and services that make the organization operate as an ongoing concern. They consider questions: "If we lost <*function*>, can we continue to operate our business and business plan(s)?" An example of this exercise may be similar to: "If we lost our <*website*>, could we still deliver services to our customers?" * Once this team has answered the questions for *every function* that is performed in the organization, then *every function* can be prioritized based on criticality and business value. * Once these critical functions are prioritized, then the systems, applications, networks, storage, databases, and technical resources that support these *highest priority functions* can be identified and prioritized as well, based on their criticality and business value. * An organization may identify the critical information system components and their functions for developing an impact analysis in the case of failure. **Technology Requirement(s):**	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14

			Once the highest priority functions and their corresponding supporting technical resources are prioritized, it is imperative that spare equipment, circuit boards, parts, fuel, circuits, servers, and anything physical and technical that can minimize outages and downtime of critical systems, be procured. These critical spares should be stored where operational staff can quickly access and install in order to minimize any outages or downtime of critical systems. **Barriers:** *The Operational requirements to prioritize critical functions and critical systems and resources will require assigning and allocating staff (that may be assigned to other functions), to document this prioritization and to keep it updated with business and personnel changes. *There will be a CAPEX cost of procuring critical spares, and there will be an OPEX cost to obtaining adequate storage space for and maintaining environmental conditions for critical spares.	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**Operational Requirement(s):** Organizational leadership, operations and engineering staff can determine who (by job function) needs to know what information within the entire organization. Following this exercise, various levels of cybersecurity responsibilities and leadership can be assigned. These levels of cybersecurity responsibilities will include but not limited to: Security of entire infrastructure, security of groups of systems/applications/databseses/SW/devices, security of individual systems/applications/databseses/SW/devices, as well as security of internal and external communications channels. The cybersecurity leadership can then develop cybersecurity policies and procedures, then train the appropriate staff of these cybersecurity procedures. **Technology Requirement(s):** Documented roles and responsibilities can be stored and accessible, where all of the organization's staff can read, download and print. **Barriers:**	· **COBIT 5** APO01.02, DSS06.03 · **ISO/IEC 27001:2013** A.6.1.1 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

			*The Operational requirements to assign cybersecurity leadership and responsibilities may require the additional cost of hiring specialized personnel and/or assigning cybersecurity responsibilities to staff (that may be assigned to other functions). These cybersecurity responsibilities, policies and procedures will constantly need updating to keep pace with business changes, evolving security climates and personnel changes. * The roles and responsibilities will need buy-in, approval from all levels of leadership, including the executive levels of the organization.	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**Operational Requirement(s):** Organizational leadership, operations and engineering staff can determine how the organization fits into a supply chain ecosystem. The following questions can be answered: *Is the organization a producer, a consumer, both, or something that has yet to be defined? Does the organization turn raw materials into a product? Does the organization provide a service where human resources and expertise is the main ingredient for business operations? Is the organization in the middle of a larger supply chain ecosystem? How does the organization earn revenue from it's customers? How does the sales function get what it needs to sell a product or service to customers?* * The organization should understand and communicate its role, responsibilities and criticality within a supply chain ecosystem to its entire staff. * The sub-organizations that are deemed critical to operating the business must be prioritized such that key decision makers are very aware of their responsibilities and available human and physical resources. This sub-organization prioritization can also be conveyed to the entire staff in such a way that every person know whom (internally and externally) to take direction from. * Once the organizational prioritization exercise is completed, the critical dependencies of all sub-organizations and outside external sources can be identified, such that the transfer of information and resources can be prioritized as well, both internally and externally to the main organization. * Organizations can develop a system to validate that supplies are genuine; reviewing the supplier processes before engaging in business. **Technology Requirement(s):**	· **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12

			Once the supply chain roles and responsibilities are identified, conveyed and in place, the key information that can transfer between various sub-organizations, organizations, and its external sources can be developed, enhanced, improved or updated to meet the critical business communications requirements within a supply chain ecosystem. The critical networks, protocols, web services, forms, emails, VPNs, VLANs, WANs, databases, web portals that can transfer critical information between various sub-organizations, organizations, and it's external sources can be developed, enhanced, improved or updated to meet the critical business requirements within a supply chain ecosystem. * This technical architecture supporting an organization's role in the supply ecosystem can also be conveyed to the appropriate technical, operations and leadership staff. **Barriers:** The organization or its external interfacing partners may not agree on the critical functions or priority. If a downstream entity is not secure or doesn't maintain a certain level of quality, it could make an upstream entity vulnerable unintentionally if they both do not agree on criticality and priority of their respective functions. The roles and responsibilities will need buy-in, approval from all levels of the supply chain, including their executive levels of their organizations.	
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**Operational Requirement(s):** Organizational leadership, operations and engineering staff may determine how the organization fits into a *Critical Infrastructure* ecosystem. The following questions can be answered: *Does this organization supply a product or service to critical infrastructure that supports the functioning of our society or economy? Does this organization supply a product or service to the government to support the security of our society or economy?* * The organization should understand and communicate its role, responsibilities and criticality within a *Critical Infrastructure* ecosystem to its entire staff. The sub-organizations that are deemed critical to operating the business can be prioritized such that key decision makers are very aware of their responsibilities and available human and physical resources. This sub-organization prioritization can also be conveyed to the entire staff in such a way that every person know whom (internally and externally) to take direction from. * Once the organizational prioritization exercise is	· **COBIT 5** APO02.06, APO03.01 · **NIST SP 800-53 Rev. 4** PM-8

			completed, the critical dependencies of all sub-organizations and outside external sources can be identified, such that the transfer of information and resources can be prioritized as well, both internally and externally to the main organization. * Organizations may address information security issues within the Critical Infrastructure Protection Plan (CIPP) that may be required by federal laws, policies, and regulations. **Technology Requirement(s):** Once the *Critical Infrastructure* roles and responsibilities are identified, conveyed and in place, the key information that can transfer between various sub-organizations, organizations, and its external sources can be developed, enhanced, improved or updated to meet the critical business communications requirements within a supply chain ecosystem. The critical networks, protocols, web services, forms, emails, VPNs, VLANs, WANs, databases, web portals that can transfer critical information between various sub-organizations, organizations, and it's external sources can be developed, enhanced, improved or updated to meet the critical business requirements within a *Critical Infrastructure* ecosystem. This technical architecture supporting an organization's role in the *Critical Infrastructure* ecosystem can also be conveyed to the appropriate technical, operations and leadership staff. **Barriers:** The organization or its external interfacing partners may not agree on the organization's criticality or priority within the critical infrastructure ecosystem. If a downstream entity is not secure or doesn't maintain a certain level of quality, it could make an upstream entity vulnerable unintentionally, resulting in an undesirable compromise and mitigation strategies may have to be devised and implemented to compensate.	

		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**Operational Requirement(s):** Organizational leadership, operations and engineering staff can determine the organization's mission and its primary business objectives as an ongoing concern. The sub-organizations that are deemed critical to operating the business can be prioritized such that key decision makers are very aware of their responsibilities and available human and physical resources. * This sub-organization prioritization can also be conveyed to the entire staff in such a way that every person know whom (internally and externally) to take direction from. * Once the organizational prioritization exercise is completed, the critical dependencies of all sub-organizations and outside external sources can be identified, such that the transfer of information and resources can be prioritized as well, both internally and externally to the main organization. An organization can identify the critical information system components and their functions for developing an impact analysis in the case of failure. **Technology Requirement(s):** None **Barriers:** * The organization and/or its leadership may find difficulty and challenges to overcome in obtaining full buy-in to its mission, objectives and subsequent policies and procedures. *	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**Operational Requirement(s):** Organizational leadership, operations and engineering staff can determine critical functions for delivery of critical services. * Then they can determine what resources, products, services, and materials that are critical and required and that they depend upon obtaining from 3rd party entities. An example would be similar to a telecom network operator who depends on a diesel fuel supplier to bring fuel to a network node site or data center as often as required during the loss of commercial power, so the telecom network operator can keep its critical network systems operating on back-up generator power. * Dependencies supporting critical functions can include but not limited to: diesel fuel, alternate sources of electricity, alternate and	· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14

			redundant communications service providers, spare components, emergency responders, vendor-crisis response teams and equipment, government agencies etc. **Technology Requirement(s):** Primary, secondary and tertiary communications systems and techniques can be implemented, so that the organization can reach its critically dependent 3rd party entities in an emergency and/or crisis situation. These modes of communication include but limited to telephony, VoIP, IM, Video conference, Internet/Email, Text/SMS and possibly Social media as modes of critical communications. **Barriers:** The organization may incur additional expenses implementing the various modes of redundant communications. The organization may incur expenses develop emergency communications procedures and to train personnel on how to use them. The identified 3rd party entities that organizations depend upon may have additional obligations or different priorities, such that they may not meet the organization's expectations as rapidly as required in the event of an emergency or crisis.	
		ID.BE-5: Resilience requirements to support delivery of critical services are established	**Operational Requirement(s):** Once the organizational leadership, operations and engineering staff has determined critical functions for delivery of critical services. Then they ~~can~~ determine redundant, sometimes duplicative methods for delivery of critical components, supplies and materials. This may include but not limited to redundant circuits for communications, alternate secondary suppliers of fuel, secondary suppliers of critical components, secondary shipping and delivery providers, alternate means of communicating with government officials and first responders. * An organization may develop a contingency plan that outlines the process for restoring information systems, and implements an	· **COBIT 5** DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

			alternative processes in the interim. This could include a plan that identifies critical assets, alternate processing/storage site, and coordinates with external service providers. **Technology Requirement(s):** Primary, secondary and tertiary communications systems and techniques can be implemented, so that the organization can reach its critically dependent 3rd party entities in an emergency and/or crisis situation. These modes of communication include but limited to telephony, VoIP, IM, Video conference, Internet/Email, Text/SMS, and possibly Social media as a last resort of critical communications. All of these modes of communications can be made as secure as practically possible and include authentication functions. **Barriers:** The organization may incur additional expenses implementing the various modes of redundant communications. The organization may incur expenses develop emergency communications procedures and to train personnel on how to use them. The identified 3rd party entities that organizations depend upon may have additional obligations or different priorities, such that they may not meet the organization's expectations as rapidly as required in the event of an emergency or crisis.	
	Governance	**ID.GV-1:**	**Operational Requirement(s):**	· **COBIT 5**

	(ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Organizational information security policy is established	An organization's executive and technical leadership can determine which information and data types that can be protected from threats. Critical financial and technical data may be protected and secured from unauthorized access and can address privacy considerations. Other types of information may be allowed to reach certain people on a need-to-know basis, in order to perform their jobs. * While some less-critical types of information may be allowed to reach the public or the media. Once these levels of information are determined, the amount of security and security controls applied to each information type can be determined. * From here, an organization can produce a set of security policies that protects critical organizational information. Once the information security policies are established, these policies can be conveyed to the appropriate levels of staffing, and external entities such that everyone knows their responsibilities in protecting various types of information. **Technology Requirement(s):** Documented Security policy, along with roles and responsibilities can be stored and accessible, where all of the organization's staff can read, download and print. **Barriers:** There may be disagreement and efforts to reconcile within organization as what level of protection is required for each data type and there may be disagreement on access control that dictates whom shall have access to what data.	APO01.03, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	**Operational Requirement(s):** Once the information security policies are established within an organization, these policies can be conveyed to the appropriate levels of executives, management, and staffing, such that everyone knows their responsibilities in protecting various types of information. External policies and procedures for protecting information can also be developed. These externally facing information security policies and procedures can also be strongly conveyed to external suppliers, partners, peers and 3rd party entities that support the organization.	· **COBIT 5** APO13.12 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 · **NIST SP 800-53 Rev. 4** PM-1, PS-7

			Technology Requirement(s): None **Barriers:** The identified 3rd party entities that organizations depend upon, may have additional obligations or different priorities, such that they may not meet the organization's information security requirements and policies as thoroughly as desired by the organization. There may be disagreement and efforts to reconcile within organization as to what level of protection is required for each data type and there may be disagreement on access control that dictates whom shall have access to what data.	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**Operational Requirement(s):** An organization's executive and technical leadership can include the organization's legal counsel and/or legal staff in the development of cybersecurity and information protection policies. They can ensure that these new cybersecurity and information protection policies conform to and do not violate privacy laws and civil liberties obligations. Once the legal details of the cybersecurity and information protection policies are established, they can be conveyed to the entire organization's staff. Staff confirmation and possibly acceptance of these cybersecurity and information protection policies may need to be obtained. Non-acceptance by certain individuals, may dictate what responsibilities are assigned to them. **Technology Requirement(s):** None **Barriers:** Some 'desired' cybersecurity and information protection requirements may conflict with the legal rights of individuals employed by the organization. Staff confirmation and possibly acceptance of these cybersecurity and information protection policies may need to be obtained. Non-acceptance by	· **COBIT 5** MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1 · **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)

			certain individuals, may dictate what responsibilities are assigned to them.	
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**Operational Requirement(s):** Once an organization creates an ongoing Threats/Risk catalog, they may progress to developing the appropriate cyber risk management responses by all of the sub-organizations that play a role of managing and responding to these risks. These appropriate responses, may include, but not be limited to the 5 phases of emergency management; Prevention, Mitigation, Preparedness, Response, and Recovery. The appropriate responses may describe "Who does What, and When" for every identified risk in the risk catalog. These responses can include every sub-organization from the top executives all the way through to the most remote member of an organization. **Technology Requirement(s):** Documented Security policy along with roles and responsibilities may be stored and accessible, where all of the organization's staff can read, download and print. **Barriers:** There may be disagreement and efforts to reconcile within the organization as to what level of protection is required for each data type and there may be disagreement on access control that dictates whom shall have access to what data.	· **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Risk Assessment	**ID.RA-1:** Asset	**Operational Requirement(s):**	· **CCS CSC** 4

	(ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	vulnerabilities are identified and documented	Technical staff may research publicly available information and vendor proprietary information to learn of all of the publicly-known vulnerabilities of the critical hardware, software, database and network resources of an organization. The technical staff may also research cyber-criminal elements for vulnerabilities that are not public or known by the vendors. Once documented and key organizational decision makers can be alerted. Technical staff may subscribe to websites and news boards that exist for the sole purpose of spreading details of found technical vulnerabilities over the Internet. An organization may outline what systems should be monitored, the frequency at which to monitor them, perform security assessments of these systems, and report all findings. An organization can conduct an assessment of risk by taking into account the magnitude of harm caused from the breach of the information system. This includes taking into account the threats, vulnerabilities, likelihood, and impact to organizational operations and assets. etc. This assessment would also include risk from external parties. Create a patch and vulnerability group (PVG) who are tasked with the job of implementing the vulnerability management program. The organization may develop a system to receive info. about security alerts, advisories, and directives. Also, develop a system that disseminates internal security alerts, advisories, and directives. **Technology Requirement(s):** When organizations perform penetration testing using a reliable set of penetration test technologies testing along with pretest analysis on the target system, in order to identify vulnerabilities based upon this analysis, and design testing to try and exploit vulnerability. An organization may employ vulnerability scanning tools that include the capability to readily detect new vulnerabilities. An organization may look to external expertise to perform independent testing of critical infrastructure under the appropriate and relevant service level and security agreements. **Barriers:** *Professional staff can be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust can be established and additional levels of training can take place.	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

			* The vendors may not accept found vulnerabilities, or they may not fix/solve their vulnerabilities before the organization is compromised by an attack of discovered vulnerabilities. * Researching for vulnerabilities may lead various staff members to access illegal or criminally backed websites, possibly violating cybersecurity and information protection policies.	
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**Operational Requirement(s):** Technical staff may research publicly available information and vendor proprietary information to learn of all of the publicly-known vulnerabilities of the critical hardware, software, database and network resources of an organization. * The technical staff may also research cyber-criminal elements for vulnerabilities that are not public or known by the vendors. All of these vulnerabilities can be documented and key organizational decision makers can be alerted. Technical staff should subscribe to websites and news boards that exist for the sole purpose of spreading details of found technical vulnerabilities over the Internet. * An organization may outline what systems should be monitored, the frequency at which to monitor them, perform security assessments of these systems, and report all findings. An organization may conduct an assessment of risk by taking into account the magnitude of harm caused from the breach of the information system. This includes taking into account the threats, vulnerabilities, likelihood, and impact to organizational operations and assets. etc. This assessment would also include risk from external parties. * Create a patch and vulnerability group (PVG) who are tasked with the job of implementing the vulnerability management program. The organization may develop a system to receive info. about security alerts, advisories, and directives. Also, develop a system that disseminates internal security alerts, advisories, and directives. * The organization establishes and institutionalizes contact with selected groups and associations within the cyber security community. * The organization implements a threat awareness program that includes a cross-organization information-sharing capability. * The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. **Technology Requirement(s):**	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5

			The organization can implement automated information feeds from external sources, like RSS, Message Boards, Twitter, Google "Search" filters etc., and any other means of receiving electronic updates on new cyber threats and attacks. These automated information feeds may include new information on equipment, software, databases, web applications and open-source software that the organization has in in place. * The organization can also implement an internal reporting policy and process, so employees can anonymously report suspicious activities. * Once these new threats and vulnerabilities are received, the organization can document and distribute to the appropriate personnel in a timely manner, so that decision makers can choose to take action. **Barriers:** The chosen sources, to which threats and vulnerabilities can be drawn from, may violate the organization cybersecurity policies and procedures. The organization should use extreme caution and ensure that these sources do not connect directly to critical networks and systems. They should be used as information sources only. Professional staff may be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust may be established and additional levels of training can take place.	
		ID.RA-3: Threats,	**Operational Requirement(s):**	· **COBIT 5**

		both internal and external, are identified and documented	Technical staff may research publicly available information and vendor proprietary information to learn of all of the publicly-known vulnerabilities of the critical hardware, software, database and network resources of an organization. * The technical staff may also research cyber-criminal elements for vulnerabilities that are not public or known by the vendors. All of these vulnerabilities should be documented and key organizational decision makers can be alerted. Technical staff should subscribe to websites and news boards that exist for the sole purpose of spreading details of found technical vulnerabilities over the Internet. * An organization should outline what systems should be monitored, the frequency at which to monitor them, perform security assessments of these systems, and report all findings. An organization may conduct an assessment of risk by taking into account the magnitude of harm caused from the breach of the information system. This includes taking into account the threats, vulnerabilities, likelihood, and impact to organizational operations and assets. etc. This assessment would also include risk from external parties. * Create a patch and vulnerability group (PVG) who are tasked with the job of implementing the vulnerability management program. The organization should develop a system to receive info. about security alerts, advisories, and directives. Also, develop a system that disseminates internal security alerts, advisories, and directives. * The organization establishes and institutionalizes contact with selected groups and associations within the cyber security community. * The organization implements a threat awareness program that includes a cross-organization information-sharing capability. * The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. **Technology Requirement(s):** The organization may implement automated information feeds from external sources, like RSS, Message Boards, Twitter, Google "Search" filters etc., and any other means of receiving electronic updates on new cyber threats and attacks. These automated information feeds may include new information on equipment, software, databases, web applications and open-source software that the organization has in in place. * The organization can also implement an internal reporting policy and process, so employees can anonymously report suspicious activities. * Once these new threats and vulnerabilities are received, the organization can document and distribute to the	APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16

			appropriate personnel in a timely manner, so that decision makers can choose to take action. **Barriers:** Professional staff should be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust can be established and additional levels of training can take place. Researching for vulnerabilities may lead various staff members to access illegal or criminally backed websites, possibly violating cybersecurity and information protection policies. The chosen sources, to which threats and vulnerabilities can be drawn from, may violate the organization cybersecurity policies and procedures. The organization should use extreme caution and ensure that these sources do not connect directly to critical networks and systems. They should be used as information sources only.	
		ID.RA-4: Potential	**Operational Requirement(s):**	· **COBIT 5**

		business impacts and likelihoods are identified	Organizational leadership, operations and engineering staff may determine the primary-critical functions and services that make the organization operate as an ongoing concern. They can ask the questions: "If we lost <function>, can we continue to operate our business and business plan(s)?" An example of this exercise may be similar to: "If we lost our <website>, could we still deliver services to our customers?" * Once this team has answered the questions for every function that is performed in the organization, then every function can be prioritized based on criticality and business value. Once these critical functions are prioritized, then the systems, applications, networks, storage, databases, and technical resources that support these highest priority functions can be identified and prioritized as well, based on their criticality and business value. * An organization identifies the critical information system components and their functions for developing an impact analysis in the case of failure. * An organization can identify the critical information system components and their functions for developing an impact analysis in the case of failure. Organizational leadership, operations and engineering staff can determine critical functions for delivery of critical services. * Then they can determine what resources, products, services, and materials that are critical and required and that they depend upon obtaining from 3rd party entities. An example would be similar to a telecom network operator who depends on a diesel fuel supplier to bring fuel to a network node site or data center as often as required during the loss of commercial power, so the telecom network operator can keep its critical network systems operating on back-up generator power. Dependencies supporting critical functions can include but not limited to: diesel fuel, alternate sources of electricity, alternate and redundant communications service providers, spare components, emergency responders, vendor-crisis response teams and equipment, government agencies etc. **Technology Requirement(s):** None **Barriers:** The organization and/or its leadership may find difficulty and a challenge to overcome in obtaining full buy-in to the identified business impacts, likelihoods and critical systems and resources.	DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14

		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**Operational Requirement(s):** The organization may build a list, chart or table to identify threats and vulnerabilities to the critical business functions, their systems, their networks and their software. * Organizations can also determine if these threats and vulnerabilities increase or decrease risk occurrences. An example would list network, hardware, and software resources you need to accomplish a business task. * Then, in a second column, list the threats associated with each resource. In a third column, list/describe the consequences of each threat. Once this threat information is established, the organization can prioritize the criticality of each risk to the business operations and the urgency and time required to respond. * The organization may categorize and prioritize these risks, so decision makers can take appropriate and efficient action. An example, organizations often develop plans to respond to physical threats, such as malicious access to buildings or equipment, and electronic threats, such as cyber-attacks trying to access sales data or computer viruses, worms or other infections, and technical failures, such as equipment failures or unexpected downtime due to power interruptions. The list of threats and vulnerabilities can also include human error. Mistakes could cause catastrophic data loss. * Create a risk catalog document, which acts as a permanent record of concerns. Use the risk catalog as a checklist to review risks on a regular on-going basis. **Technology Requirement(s):** None **Barriers:** The organization and/or its leadership may find difficulty obtaining full buy-in to the identified business impacts, likelihoods and critical systems and resources. The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

		ID.RA-6: Risk responses are identified and prioritized	**Operational Requirement(s):** Once an organization creates an ongoing Threats/Risk catalog, they may progress to developing the appropriate cyber risk management responses by all of the sub-organizations that play a role of managing and responding to these risks. These appropriate responses, may include, but not be limited to the 5 phases of emergency management; PREVENTION, MITIGATION, PREPAREDNESS, RESPONSE, and RECOVERY. The appropriate responses may describe "Who does What, and When" for every identified risk in the risk catalog. These responses may include every sub-organization from the top executives all the way through to the most remote member of an organization. **Technology Requirement(s):** None **Barriers:** There may be disagreement within organization and a need to reconcile as to what responses are required and by whom.	· **COBIT 5** APO12.05, APO13.02 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**Operational Requirement(s):** The appropriate cyber risk management responses, may include, but not be limited to the 5 phases of emergency management; PREVENTION, MITIGATION, PREPAREDNESS, RESPONSE, and RECOVERY. The appropriate responses should describe "Who does What, and When" for every identified risk in the risk catalog. These responses should include every sub-organization from the top executives all the way through to the most remote and junior member of an organization. These responses can also include the timeliness of each response, to include, but not limited to immediate responses through, timelines needed based on dependencies. **Technology Requirement(s):** None	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009 4.3.4.2** · **NIST SP 800-53 Rev. 4 PM-9**

			Barriers: There may be disagreement within organization and a need to reconcile as to what responses are required and by whom. There may be OPEX and CAPEX costs associated with implementing the Risk Management Plans and Processes	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**Operational Requirement(s):** The appropriate cyber risk management responses, may include, but not be limited to the 5 phases of emergency management; PREVENTION, MITIGATION, PREPAREDNESS, RESPONSE, and RECOVERY. The appropriate responses may describe "Who does What, and When" for every identified risk in the risk catalog. These responses can include every sub-organization from the top executives all the way through to the most remote member of an organization. These responses may also include the timeliness of each response, to include, but not limited to immediate response through, timelines needed based on dependencies. * Organizations, sub-organizations and all data owners who manage and maintain information technology assets may receive comprehensive training on implementing cybersecurity best practices. * Organization may determine the consequences of various cyber incidents. These consequences should include, but not limited to impact to supply chain / degradation of public trust / financial and market losses / degradation of brand reputation / impact to critical infrastructure. **Technology Requirement(s):** None **Barriers:** There may be disagreement within organization and a need to reconcile as to what responses are required and by whom. There may be OPEX and CAPEX costs associated with implementing the Risk Management Plans and Processes	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The	**Operational Requirement(s):**	· **NIST SP 800-53**

		organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Organizational leadership, operations and engineering staff may determine how the organization fits into a *Critical Infrastructure* ecosystem. The following questions should be answered: *Does this organization supply a product or service to critical infrastructure that supports the functioning of our society or economy? Does this organization supply a product or service to the government to support the security of our society or economy?* The organization may understand and communicate its role, responsibilities and criticality within a *Critical Infrastructure* ecosystem to its entire staff. The sub-organizations that are deemed critical to operating the business can be prioritized such that key decision makers are very aware of their responsibilities and available human and physical resources. This sub-organization prioritization must also be conveyed to the entire staff in such a way that every person know whom (internally and externally) to take direction from. * Once the organizational prioritization exercise is completed, the critical dependencies of all sub-organizations and outside external sources can be identified, such that the transfer of information and resources can be prioritized as well, both internally and externally to the main organization. Address information security issues within the Critical Infrastructure Protection Plan (CIPP) that may be required by federal laws, policies, and regulations. * The organization can build a list, chart or table to identify threats and vulnerabilities to *their critical infrastructure functions*, their systems, their networks and their software that supports critical infrastructure. Organizations can also determine if these threats and vulnerabilities increase or decrease risk occurrences. An example would list network, hardware, and software resources you need to accomplish a business task. Then, in a second column, list the threats associated with each resource. In a third column, list/describe the consequences of each threat. * Once this threat information is established, the organization can prioritize the criticality of each risk to the critical infrastructure functions and the urgency and time required to respond. * The organization can categorize and prioritize these risks, so decision makers can take appropriate and efficient action. An example, organizations often develop plans to respond to physical threats, such as malicious access to buildings or equipment, and electronic threats, such as cyber-attacks trying to access sales data or computer viruses, worms or other infections, and technical failures, such as equipment failures or unexpected downtime due to power interruptions. The list of threats and vulnerabilities must also include human error. Mistakes could cause catastrophic data loss. * Create a risk catalog document,	**Rev. 4** PM-8, PM-9, PM-11, SA-14

which acts as a permanent record of concerns. Use the risk catalog as a checklist to review risks on a regular on-going basis.

Technology Requirement(s):

Once the *Critical Infrastructure* roles and responsibilities are identified, conveyed and in place, the key information that should transfer between various sub-organizations, organizations, and its external sources can be developed, enhanced, improved or updated to meet the critical business communications requirements within a supply chain ecosystem. The critical networks, protocols, web services, forms, emails, VPNs, VLANs, WANs, databases, web portals that can transfer critical information between various sub-organizations, organizations, and it's external sources can be developed, enhanced, improved or updated to meet the critical business requirements within a *Critical Infrastructure* ecosystem. This technical architecture supporting an organization's role in the *Critical Infrastructure* ecosystem,

			may also be conveyed to the appropriate technical, operations and leadership staff. **Barriers:** The organization or its external interfacing partners may not agree on the organization's criticality or priority within the critical infrastructure ecosystem. If a downstream entity is not secure or doesn't maintain a certain level of quality, it could make an upstream entity vulnerable unintentionally, resulting in an undesirable compromise.	
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**Operational Requirement(s):** The organization can determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization can take into account "all" internal communications with: *Tiers I, II, III of critical infrastructure related operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc.* Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. The entire flow of information that describes who-what-when-how must be documented and conveyed through ongoing training, to the effected personnel. The organization can determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. The organization must take into account "all" external communications with: vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc. Once	· **CCS CSC** 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-2, IA Family

			these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. The entire flow of information that describes who-what-when-how can be documented and conveyed through ongoing training, to the effected personnel. Organization can develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. Organization can develop a baseline security compliance policy for all internal components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) **Technology Requirement(s):** Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems should all have the *authorized identities, authorized credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters should be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. **Barriers:**	

			There may be personnel in the organization that believe that their credentials have been wrongfully applied. The organization should develop business and cybersecurity rules that determine who is authorized to do what within the organization's infrastructure. If there are still disagreements and conflicts, then an organization's leadership and management should decide on a case-by-case basis. Professional staff should be allocated/assigned to this task, which 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.	
		PR.AC-2: Physical access to assets is managed and protected	**Operational Requirement(s):** The organization should determine whom within, internal and external to the entire organization, can be allowed "PHYSICAL" access to critical infrastructure networks systems, computing systems, storage systems, databases, email systems, technical spaces, data centers, wiring closets, servers rooms, devices, tools, vehicles etc. that allow the organization to be an on-going concern. These critical systems should be protected from unauthorized 'physical' access by locked doors, locked equipment cabinets, locked file and software cabinets, locked fencing, biometric locks to shared technical areas, locked vehicles, locked property and even building/landscaping designs to prevent brute-force entries to critical areas. **Technology Requirement(s):** The entire physical protection environment should be monitored and managed by an automated, easy to use system that can see and detect entry by authorized and unauthorized persons. This automated physical protection management system should also have the integrated ability to allow authorized operations personnel (i.e.; a NOC) to visibly see critical/protected assets, collect/store/playback video of protected assets, lock and unlock physical assets, doors, entry ways, vehicles etc., remotely. **Barriers:** Professional staff should be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust can be established and additional levels of training can take place.	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9

			There will be a CAPEX cost associated with procuring, installing and managing a physical protection management system. There will be a time element associated with evaluating systems, vendors and their abilities to deliver a physical protection management system. There will be a time element to the implementation, testing, acceptance and training associated with a new physical protection management system. There will be an OPEX cost associated with allocating personnel to protect physical assets. The personnel assigned to physical protection will need to be trained on any systems that are implemented to protect physical assets, they will need to be trained to execute the organization's security and information flow plans, which includes but limited to allowing and dis-allowing other personnel from having access to physical assets.	
		PR.AC-3: Remote access is managed	**Operational Requirement(s):** The organization should determine whom within, internal and external to the entire organization, can be allowed "REMOTE" access to critical infrastructure networks systems, computing systems, storage systems, databases, email systems, technical spaces, data centers, wiring closets, servers rooms, devices, tools, vehicles etc. that allow the organization to be an on-going concern. These critical systems should be protected from unauthorized 'REMOTE' access by mechanisms including, but not limited to: firewalls, USERNAME/PASSWORDs, mult-factor identification, access control lists, scheduling limits, VPN access, LAN/WAN access, biometrics, encryption keys etc. **Technology Requirement(s):** The entire remote protection environment should be monitored and managed by an automated, easy to use REMOTE ACCESS system that can see and detect entry by authorized and unauthorized persons and activity. This automated REMOTE ACCESS protection management system, should also have the integrated ability to allow authorized operations personnel (i.e.; a NOC) to visibly see who is doing what from outside the physical confines of the organization and at a virtual level. Authorized operations personnel can also be able to see what 'virtual' activity is taking place, like login attempts, remote port scans, database injections, software and file modifications, storage system accesses, unauthorized remote communications etc.	· **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20

			Barriers: There will be a CAPEX cost associated with procuring, installing and managing a REMOTE ACCESS protection management system. There will be a time element associated with evaluating systems, vendors and their abilities to deliver a physical protection management system. There will be a time element to the implementation, testing, acceptance and training associated with a new REMOTE ACCESS protection management system. There will be an OPEX cost associated with allocating personnel to protect assets from REMOTE ACCESS. The personnel assigned to REMOTE ACCESS protection will need to be trained on any systems that are implemented to protect assets from unauthorized REMOTE ACCESS, they will need to be trained to execute the organization's security and information flow plans, which includes but limited to allowing and dis-allowing other personnel from having REMOTE access to physical assets.	
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**Operational Requirement(s):** Organization may implement an Access-Permission policy based on Separation of duties and Least Privilege. Separation of duties requires dividing all organizational functions among multiple people to limit the possibility that one employee could harm an organization without the cooperation of others. In general, employees are less likely to engage in malicious acts if they should collaborate with other employees. Ideally, organizations may include separation of duties in the design of their business processes and enforce these processes through technical and nontechnical means. The separation of duties policy also requires implementation of least privilege, which means authorizing people to use only the resources needed to do their job. * Organizations often manage least privilege as an ongoing process, particularly when employees move through the organization as a result of promotions, transfers, relocations, demotions, and especially terminations. These privileges can be controlled using physical, administrative, and technical procedures and systems. Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber-attack. These principles apply in both the physical and virtual worlds where organizations need to prevent employees from gaining physical or online access to resources not required by their work roles. * The organization can carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove	· **CCS CSC** 12, 15 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16

			permissions that are no longer needed. The organization can establish account management policies and procedures and regularly audit account activity. **Technology Requirement(s):** The organization may implement automated access control to systems, servers, access doors etc. to limited unauthorized access and only allow those who can successfully show their valid and up-to-date credentials. * These automated access control system(s) may lock down assets when unauthorized access attempts are detected and when there are a number of failed attempts to enter in credentials. * A best practice for access control is based on a multi-level series of gates one can pass to allow access and an access policy based on Least Privilege-Separation of Duties parameters. **Barriers:** The implementation of separation of duties and least privileges will require allocation of qualified personnel to perform this function and enforce the rules. Implementing these practices at a granular level may also interfere with business processes. Most organizations find it challenging to strike a balance between implementing these recommendations and accomplishing the organization's mission. Professional staff should be allocated/assigned to this task, which 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.	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**Operational Requirement(s):** The organization's technical and operations staff may design their critical infrastructure networks, such that they can withstand attacks, nodal failures and resources outages. A suggested approach is to segment the network design into smaller segments, so if an anomaly occurs at one location or node, it can be isolated and not take down the entire network. It is understood that segmentation may not be applicable to all network scenarios, but it should be considered by the organization and evaluated for its ability to maintain network integrity. Alternatives to network segmentation may be explored in order to achieve comparable levels of resiliency. **Technology Requirement(s):** The overall network design may be designed to maintain the fullest, maximum practical operational integrity. The network design should employ maximum practical diversity, redundancy, and segmentation where it is practical. **Barriers:** There will be an added CAPEX and OPEX cost to deploying diverse, redundant and segmented network designs, in order to protect and maintain network integrity at all times. The organization will have to weigh the costs vs. the risks of losing the network and its business, and decide to implement network designs based on their risk tolerance.	· **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, SC-7
	Awareness and	**PR.AT-1:** All users	**Operational Requirement(s):**	· **CCS CSC** 9

	Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	are informed and trained	Organizational leadership, operations and engineering staff should determine who (by job function) needs to know what information within the entire organization. Following this exercise, various levels of cybersecurity responsibilities and leadership can be assigned. These levels of cybersecurity responsibilities will include but not limited to: Security of entire infrastructure, security of groups of systems/applications/databseses/SW/devices, security of individual systems/applications/databseses/SW/devices, as well as security of internal and external communications channels. The cybersecurity leadership can then develop cybersecurity policies and procedures, then train the appropriate staff of these cybersecurity procedures. Once the information security policies are established within an organization, these policies should be conveyed to the appropriate levels of executives, management, and staffing, such that everyone knows their responsibilities in protecting various types of information. External policies and procedures for protecting information, may also be developed. These externally facing information security policies and procedures should also be strongly conveyed to external suppliers, partners, peers and 3rd party entities that support the organization. **Technology Requirement(s):** None **Barriers:** The Operational requirements to assign cybersecurity leadership and responsibilities may require the additional cost of hiring specialized personnel and/or assigning cybersecurity responsibilities to staff (that may be assigned to other functions). These cybersecurity responsibilities, policies and procedures will constantly need updating to keep pace with business changes, evolving security climates and personnel changes. The identified 3rd party entities that organizations depend upon, may have additional obligations or different priorities, such that they may not meet the organization's information security requirements and policies as thoroughly as desired by the organization.	· **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged	**Operational Requirement(s):**	· **CCS CSC** 9

		users understand roles & responsibilities	* The organization may determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization can take into account "all" internal communications with: Tiers I,II,III of critical infrastructure related operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. * Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how can be documented and conveyed through ongoing training, to the effected personnel. * The organization should determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. * The organization may take into account "all" external communications with: vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc. Once these communication paths and flows have been determined the organization should set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * Organization may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. * Organization may develop a baseline security compliance policy for all internal components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) * The Organization may implement an Access-Permission policy based on ***Separation of duties*** and ***Least Privilege***. Separation of duties requires dividing all organizational functions among multiple people to limit the possibility that one employee could harm an organization without the cooperation of others. In general, employees are less likely to engage in malicious acts if they should collaborate with other employees. Ideally, organizations should include separation of duties in the design of their business processes and enforce these processes through technical and nontechnical means. The separation of duties policy also requires implementation of least privilege, which means authorizing people to use only the resources needed to do their job. * Organizations may	· **COBIT 5** APO07.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13

manage least privilege as an ongoing process, particularly when employees move through the organization as a result of promotions, transfers, relocations, demotions, and especially terminations. These privileges can be controlled using physical, administrative, and technical procedures and systems. Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber attack. These principles apply in both the physical and virtual worlds where organizations need to prevent employees from gaining physical or online access to resources not required by their work roles. * The organization should carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove permissions that are no longer needed. The organization should establish account management policies and procedures and regularly audit account activity. Once these access-permission policies and procedures are established, all personnel may be trained and continuously reminded of their roles, responsibilities and any enforceable actions that can occur, should there be any intentional violations.

Technology Requirement(s):

			Organizations, sub-organizations and all data owners who manage and maintain information technology assets may receive comprehensive training on implementing cybersecurity best practices. **Barriers:** The implementation of separation of duties and least privileges will require allocation of qualified personnel to perform this function and enforce the rules. Implementing these practices at a granular level may also interfere with business processes. Most organizations find it challenging to strike a balance between implementing these recommendations and accomplishing the organization's mission. There may be gaps in the training and conveyance of information, regarding cyber security roles and responsibilities. This may in turn lead to undesirable organizational consequences and negative impacts on the critical systems, networks and resources.	
		PR.AT-3: Third-party	**Operational Requirement(s):**	· **CCS CSC** 9

		stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	* The organization may determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization may take into account "all" internal communications with: Tiers I,II,III of critical infrastructure related operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. * Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how should be documented and conveyed through ongoing training, to the effected personnel. * The organization may determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. * The organization may take into account "all" external communications with: vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc. Once these communication paths and flows have been determined the organization should set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * Organization may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. * Organization may develop a baseline security compliance policy for all internal components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) * The Organization may implement an Access-Permission policy based on ***Separation of duties*** and ***Least Privilege***. Separation of duties requires dividing all organizational functions among multiple people to limit the possibility that one employee could harm an organization without the cooperation of others. In general, employees are less likely to engage in malicious acts if they collaborate with other employees. Ideally, organizations can include separation of duties in the design of their business processes and enforce these processes through technical and nontechnical means. The separation of duties policy also requires implementation of least privilege, which means authorizing people to use only the resources needed to do their job. * Organizations can	· **COBIT 5** APO07.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9

manage least privilege as an ongoing process, particularly when employees move through the organization as a result of promotions, transfers, relocations, demotions, and especially terminations. These privileges can be controlled using physical, administrative, and technical procedures and systems. Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber-attack. These principles apply in both the physical and virtual worlds where organizations need to prevent employees from gaining physical or online access to resources not required by their work roles. * The organization should carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove permissions that are no longer needed. The organization may establish account management policies and procedures and regularly audit account activity. Once these access-permission policies and procedures are established, all personnel may be trained and continuously reminded of their roles, responsibilities and any enforceable actions that can occur, should there be any intentional violations.

Technology Requirement(s):

			Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems should all have the *authorized identities, authorized credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters should be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. **Barriers:** There may be personnel external to the organization (suppliers, customers, and partners) that believe that their credentials have been wrongfully applied. The organization should develop business and cybersecurity rules that determine who is authorized to do what within the organization's infrastructure. If there are still disagreements and conflicts, then an organization's leadership and management can decide on a case-by-case basis.	
		PR.AT-4: Senior	**Operational Requirement(s):**	· **CCS CSC** 9

		executives understand roles & responsibilities	* The organization may determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization may take into account "all" internal communications with: Tiers I,II,III of critical infrastructure related operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. * Once these communication paths and flows have been determined the organization should set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how may be documented and conveyed through ongoing training, to the effected personnel. * The organization can determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. * The organization may take into account "all" external communications with: vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc. Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * Organization may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. * Organization may develop a baseline security compliance policy for all internal components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) * The Organization may implement an Access-Permission policy based on ***Separation of duties*** and ***Least Privilege***. Separation of duties requires dividing all organizational functions among multiple people to limit the possibility that one employee could harm an organization without the cooperation of others. In general, employees are less likely to engage in malicious acts if they can collaborate with other employees. Ideally, organizations should include separation of duties in the design of their business processes and enforce these processes through technical and nontechnical means. The separation of duties policy also requires implementation of least privilege, which means authorizing people to use only the resources needed to do their job. * Organizations can	· **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, · **NIST SP 800-53 Rev. 4** AT-3, PM-13

			manage least privilege as an ongoing process, particularly when employees move through the organization as a result of promotions, transfers, relocations, demotions, and especially terminations. These privileges can be controlled using physical, administrative, and technical procedures and systems. Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber-attack. These principles apply in both the physical and virtual worlds where organizations need to prevent employees from gaining physical or online access to resources not required by their work roles. * The organization may carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove permissions that are no longer needed. The organization may establish account management policies and procedures and regularly audit account activity. Once these access-permission policies and procedures are established, all personnel should be trained and continuously reminded of their roles, responsibilities and any enforceable actions that can occur, should there be any intentional violations.
			Technology Requirement(s):

			Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems can all have the *authorized identities, authorized credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters should be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. **Barriers:** There may be executives within the organization that believe that their credentials have been wrongfully applied. The organization can develop business and cybersecurity rules that determine who is authorized to do what within the organization's infrastructure. If there are still disagreements and conflicts, then an organization's leadership and management should decide on a case-by-case basis.	
		PR.AT-5: Physical	**Operational Requirement(s):**	· **CCS CSC** 9

		and information security personnel understand roles & responsibilities	* The organization may determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization may take into account "all" internal communications with: Tiers I,II,III of critical infrastructure related operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. * Once these communication paths and flows have been determined the organization must set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how can be documented and conveyed through ongoing training, to the effected personnel. * The organization may determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. * The organization can take into account "all" external communications with: vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc. Once these communication paths and flows have been determined the organization can set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * Organization may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. * Organization can develop a baseline security compliance policy for all internal components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) * The Organization may implement an Access-Permission policy based on ***Separation of duties*** and ***Least Privilege***. Separation of duties requires dividing all organizational functions among multiple people to limit the possibility that one employee could harm an organization without the cooperation of others. In general, employees are less likely to engage in malicious acts if they can collaborate with other employees. Ideally, organizations can include separation of duties in the design of their business processes and enforce these processes through technical and nontechnical means. The separation of duties policy also requires implementation of least privilege, which means authorizing people to use only the resources needed to do their job. * Organizations may manage least privilege as an ongoing	· **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, · **NIST SP 800-53 Rev. 4** AT-3, PM-13

process, particularly when employees move through the organization as a result of promotions, transfers, relocations, demotions, and especially terminations. These privileges can be controlled using physical, administrative, and technical procedures and systems. Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber-attack. These principles apply in both the physical and virtual worlds where organizations need to prevent employees from gaining physical or online access to resources not required by their work roles. * The organization may carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove permissions that are no longer needed. The organization should establish account management policies and procedures and regularly audit account activity. Once these access-permission policies and procedures are established, all personnel may be trained and continuously reminded of their roles, responsibilities and any enforceable actions that can occur, should there be any intentional violations.

Technology Requirement(s):

			Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems can all have the *authorized identities, authorized credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters should be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. **Barriers:** *There may be personnel within the organization that believe that their credentials have been wrongfully applied. The organization may develop business and cybersecurity rules that determine who is authorized to do what within the organization's infrastructure. If there are still disagreements and conflicts, then an organization's leadership and management should decide on a case-by-case basis.	
	Data Security	**PR.DS-1:** Data-at-rest	**Operational Requirement(s):**	· **CCS CSC** 17

	(PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	is protected	* Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents for critical infrastructure. * Organizations with Data centers or connect with (Cloud) Data Centers should establish a benchmark of what applications reside in the datacenter. This benchmark may include, but not limited to: File activity / Authorized Access Accounts / Data flow activity / Software version control / Database snapshots / Communications ports / Protocols in use / VM quantities and activity. * Organizations should classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may consider the use of data encryption on critical classes of data, to prevent intercepted or stolen data from being read by those who are NOT authorized to have this data. * Organizations should 'Continuously' monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations should strive to REDUCE Their attack surface. The attack surface can be reduced by executing the following: Reduce the number of open ports and services on Internet-facing systems / Eliminate all unnecessary protocols and services from endpoints, servers and internal systems / Implement a least-privilege access control policy / Deploy Next Gen Firewalls to control access to applications and network resources. **Technology Requirement(s):**	· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** SC-28

			* These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking / Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. * Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems should all have the scheduling, credentials of access, business process rules, and security controls built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters may be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. **Barriers:** * There may be gaps in the training and conveyance of information, regarding cyber security roles and responsibilities. This may in turn lead to undesirable organizational consequences and negative impacts on the critical systems, networks and resources.	
		PR.DS-2: Data-in-	**Operational Requirement(s):**	· **CCS CSC** 17

		transit is protected	* Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents for critical infrastructure. * Organizations with Data centers or connect with (Cloud) Data Centers should establish a benchmark of what applications reside in the datacenter. This benchmark may include, but not limited to: File activity / Authorized Access Accounts / Data flow activity / Software version control / Database snapshots / Communications ports / Protocols in use / VM quantities and activity. * Organizations may classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may consider the use of data encryption on critical classes of data, to prevent intercepted or stolen data from being read by those who are NOT authorized to have this data. * Organizations may 'Continuously' monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. **Technology Requirement(s):** * These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking / Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. * Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems should all have the scheduling, credentials of access, business process rules, and security controls built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters may be in place that monitors file structure, metadata, or data type, thus, determining where this data may	· **COBIT 5** APO01.06, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8

			flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. * Organizations can strive to REDUCE Their attack surface. The attack surface can be reduced by executing the following: Reduce the number of open ports and services on Internet-facing systems / Eliminate all unnecessary protocols and services from endpoints, servers and internal systems / Implement a least-privilege access control policy / Deploy Next Gen Firewalls to control access to applications and network resources. **Barriers:** There may be gaps in the training and conveyance of information, regarding cyber security roles and responsibilities. This may in turn lead to undesirable organizational consequences and negative impacts on the critical systems, networks and resources.	
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**Operational Requirement(s):** Organizations can monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations can also track and document the decommissioning of equipment, systems, servers, networking equipment and ensure that all data storage capable devices are wiped clean and/or destroyed. **Technology Requirement(s):** The previously required hardware and software asset inventory systems, may have functionality to track and document disposal of assets. **Barriers:**	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:201**3 SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16

			The additional man-hours required to document before disposing critical systems, hardware and software, will likely add an additional OPEX cost to the organization.	
		PR.DS-4: Adequate capacity to ensure availability is maintained	**Operational Requirement(s):** Organizations should ensure that bandwidth, physical circuits, virtual circuits, available frequencies, computing capacity, data storage, virtual machines, and asset capacities are kept at levels that exceed the minimum required levels by 30-100%, such that failed critical infrastructure assets can have their functions shifted to working assets in order to maintain maximum desired availability. **Technology Requirement(s):** Organizations should implement maximum practical diversity, redundancy, sparing for all of their critical systems, networks and data storage. **Barriers:** * There will be additional CAPEX and OPEX costs required to procure the additional assets needed for maximum practical diversity, redundancy, and sparing. * There may be disagreement within organization as to what critical assets should be redundant, diverse and sparred.	· **COBIT 5** APO13.01 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.3.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections	**Operational Requirement(s):**	· **CCS CSC** 17

		against data leaks are implemented	* Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents on critical infrastructure. * Organizations with Data centers or connect with (Cloud) Data Centers should establish a benchmark of what applications reside in the datacenter. This benchmark may include, but not limited to: File activity / Authorized Access Accounts / Data flow activity / Software version control / Database snapshots / Communications ports / Protocols in use / VM quantities and activity. * Organizations can classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may consider the use of data encryption on critical classes of data, to prevent intercepted or stolen data from being read by those who are NOT authorized to have this data. * Organizations can 'Continuously' monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations should deploy ENDPOINT device continuous monitoring and security management functions. ENDPOINTs include but not limited to computers / servers / VMs / tablets / smartphones / storage devices / hubs / any devices that connects to the public Internet and external (Cloud) data centers. * Organizations may monitor and control critical asset configuration and installation changes. Only authorized staff and departments should be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations may also track and document the decommissioning of equipment, systems, servers, networking equipment and ensure that all data storage capable devices are wiped clean and/or destroyed. * Organizations may develop and implement a Mobile Device management and Security Plan-Policy. This plan should include but not limited to: Authorized access control / VPN Access control / Encryption control / Authorized system connections / Mobile Device Threats / Mobile Device Security testing / Mobile device patching and update frequency / Loss of Device procedures / Employee termination procedures / Employee mobile device responsibilities & rights.	· **COBIT 5** APO01.06 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

			Technology Requirement(s): Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems may all have the *scheduling, credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters may be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. * Organizations can strive to REDUCE Their attack surface. The attack surface can be reduced by executing the following: Reduce the number of open ports and services on Internet-facing systems / Eliminate all unnecessary protocols and services from endpoints, servers and internal systems / Implement a least-privilege access control policy / Deploy Next Gen Firewalls to control access to applications and network resources. **Barriers:** There may be gaps in the training and conveyance of information, regarding cyber security roles and responsibilities. This may in turn lead to undesirable organizational consequences and negative impacts on the critical systems, networks and resources. The implementation of separation of duties and least privileges will require allocation of qualified personnel to perform this function and enforce the rules. Implementing these practices at a granular level may also interfere with business processes. Most organizations find it challenging to strike a balance between implementing these recommendations and accomplishing the organization's mission.	
		PR.DS-6: Integrity	**Operational Requirement(s):**	· **ISA 62443-3-**

		checking mechanisms are used to verify software, firmware, and information integrity	* Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents on critical infrastructure. * Organizations with Data centers or connect with (Cloud) Data Centers should establish a benchmark of what applications reside in the datacenter. This benchmark may include, but not limited to: File activity / Authorized Access Accounts / Data flow activity / Software version control / Database snapshots / Communications ports / Protocols in use / VM quantities and activity. * Organizations can classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations can only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may consider the use of data encryption on critical classes of data, to prevent intercepted or stolen data from being read by those who are NOT authorized to have this data. * Organizations may 'Continuously' monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations may monitor and control critical asset configuration and installation changes. Only authorized staff and departments should be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. **Technology Requirement(s):** Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems should all have the scheduling, credentials of access, business process rules, and security controls built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters should be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your	**3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SI-7

			security safeguards from a diverse group of suppliers. **Barriers:** There may be gaps in the training and conveyance of information, regarding cyber security roles and responsibilities. This may in turn lead to undesirable organizational consequences and negative impacts on the critical systems, networks and resources. The implementation of separation of duties and least privileges will require allocation of qualified personnel to perform this function and enforce the rules. Implementing these practices at a granular level may also interfere with business processes. Most organizations find it challenging to strike a balance between implementing these recommendations and accomplishing the organization's mission.	
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**Operational Requirement(s):** Organizations should ensure that all critical infrastructure development and testing systems, servers, storage and networking assets are completely disconnected from the public Internet and completely disconnected from "Live" production-customer serving networks and systems. **Technology Requirement(s):** Separate development and testing systems, servers, storage and networking assets should be designed and built to allow new services, applications and products to be developed without being attacked, breached or stolen from unauthorized entities via the Internet. **Barriers:** There will be an additional CAPEX cost to design and build a separate development and testing environment.	· **COBIT 5** BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2

			There will be an additional OPEX cost to allocate staff to operate and maintain separate environments.	
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	**Operational Requirement(s):** * Organizations may monitor and establish BASELINE critical infrastructure network traffic, file access, database activity, software modifications, stored data access, and overall asset behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations can scan and certify all new network connected and mobile devices before they can be placed into service. * Organizations with Data centers or connect with (Cloud) Data Centers should establish a benchmark of what applications reside in the datacenter. This benchmark may include, but not limited to: File activity / Authorized Access Accounts / Data flow activity / Software version control / Database snapshots / Communications ports / Protocols in use / VM quantities and activity. * Organizations can monitor and control critical asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations can scan and certify all new network connected and mobile devices before they can be placed into service. **Technology Requirement(s):** The organization can implement a set of continuous monitoring systems and the database processing and storage assets required to handle large volumes of collected data from critical assets. * The organization can develop reports, graphs, charts and patterns that indicate what is considered normal behavior for critical assets and networks. **Barriers:** There will be an additional CAPEX cost to implement continuous monitoring systems and the associated database and storage assets required to establish a baseline and to detect deviations from the norm. There will be an additional OPEX cost to allocate staff to operate and maintain continuous monitoring systems and the associated database and storage assets required to establish a baseline and to detect deviations from the norm.	· **CCS CSC** 3, 10 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**Operational Requirement(s):** Organizations using a systems-software development lifecycle (SDLC) approach, may incorporate security into every phase of planning, analysis, design, and implementation of all of their critical infrastructure systems. * Organizations can build in security functions and procedures before, during and after they implement any of the following next-gen technologies; Software Defined Networking (SDNs), Network Function Virtualization (NFV), and Virtual Machines (VMs) . **Technology Requirement(s):** SDLC and project management tools may be implemented, based on an organization's decisions to use specific methodologies. **Barriers:** SDLC is evolving and many new development environments and project management methods are being used, like Agile, Scrum, Kanban, so there may be resistance to employing strict SDLC phases of activity.	· **COBIT 5** APO13.01 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	**Operational Requirement(s):** Organizations can monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations may also track and document the decommissioning of equipment, systems, servers, networking equipment and ensure that all data storage capable devices are wiped clean and/or destroyed. **Technology Requirement(s):** The previously required hardware and software asset inventory systems, may have functionality to track and document disposal of assets. **Barriers:**	· **COBIT 5** BAI06.01, BAI01.06 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10

			The additional human resources required to document before disposing critical infrastructure systems, hardware and software, will likely add an additional OPEX cost to the organization.	
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	**Operational Requirement(s):** Organizations may establish a critical infrastructure data and systems backup policy, and required procedures. * Once these procedures are established they can be tested, updated and then conveyed to the authorized data owners and staff. * Backups of critical data, system configurations, critical server images, virtual machine images, emails, documents, files, videos, content and information critical to the operations of the organization can be conducted on a regular basis. The frequency of back-ups is an organizational decision based on the life expectancy of the critical data and the impact to the organization if such data was lost, stolen or compromised. **Technology Requirement(s):** There should be more than adequate storage capacity, database capacity, and network bandwidth to allow frequent backups of critical information and data. * Organizations may wish to consider implementing complete full-scale disaster recovery technologies as a companion to their back-up resources. **Barriers:** There will be an additional CAPEX and OPEX cost to implement additional physical and virtual resources for conducting frequent backups and facilitating system and data recovery.	· **COBIT 5** APO13.01 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**Operational Requirement(s):** Organizations can consider building a Security Team of staff or use external security resources with the following roles included, but not limited to: Incident Responders / Digital Forensics / Investigators / Security Leadership / Compliance Auditor / Legal Professional / Security Operations * Organizations can monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC**

			departments should be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations can scan and certify all new network connected and mobile devices before they can be placed into service. **Technology Requirement(s):** None **Barriers:** There may be gaps in the training and conveyance of information, regarding cyber security roles and responsibilities. This may in turn lead to undesirable organizational consequences and negative impacts on the critical systems, networks and resources. There may be personnel within the organization that believe that their credentials have been wrongfully applied. The organization can develop business and cybersecurity rules that determine who is authorized to do what within the organization's infrastructure. If there are still disagreements and conflicts, then an organization's leadership and management should decide on a case-by-case basis.	**27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**Operational Requirement(s):** Organizations can monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations can also track and document the decommissioning of equipment, systems, servers, networking equipment and ensure that all data storage capable devices are wiped clean and/or destroyed. * Organizations may establish the acceptable life expectancy and usefulness of critical data, then establish policies and procedures to destroy data that is no longer relevant to the organization. The organization can establish and enforce controls for destroying data.	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6

			Technology Requirement(s): The previously required hardware and software infrastructure asset inventory systems, may have functionality to track and document disposal of assets. **Barriers:** The additional human resources required to document disposing critical infrastructure data for systems, hardware and software, will likely add an additional OPEX cost to the organization.	
		PR.IP-7: Protection processes are continuously improved	**Operational Requirement(s):** Organizations can strive to identify a cyber incident as rapidly as possible and reach incident containment within 1 to 4 hours. Organizations can track and measure performance times and seeks ways to reduce time to containment. * Organizations can strive to identify a cyber incident as rapidly as possible and achieve full business recovery and remediation within 1 to 24 hours. * Organizations may track and measure performance times and seeks ways to reduce time to Recovery. * Organizations may catalog lessons learned from every cyber incident. This lessons learned catalog can include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. * Organizations should be vigilant against Advance Persistent Threats (APTs) by constantly monitoring for Attacker reconnaissance / Attacker incursion / Attacker response if discovered / Attacker capture of systems / Attacker outbound communications and stolen data transfer. * Organizations may catalog lessons learned from every cyber incident. This lessons learned catalog may include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technology Requirement(s):**	· **COBIT 5** APO11.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

			Computing systems, information storage systems, databases, VPNs, LANs, VLANs,WANs, VPNs, Text/SMS, Email systems may all have the *authorized identities, authorized credentials of access, business process rules, and security controls* built into them, such that personnel and authorized external entities can access the correct information in a timely manner according to the documented communications flow. Security policy filters may be in place that monitors file structure, metadata, or data type, thus, determining where this data may flow through the information system based upon specified attributes. The system architecture is consistent with global, organization-wide information security architecture. This may include using products that subscribe to your security safeguards from a diverse group of suppliers. * Organizations can strive to REDUCE Their attack surface. The attack surface can be reduced by executing the following: Reduce the number of open ports and services on Internet-facing systems / Eliminate all unnecessary protocols and services from endpoints, servers and internal systems / Implement a least-privilege access control policy / Deploy Next Gen Firewalls to control access to applications and network resources. * Organizations may consider the use of "Sandboxing" or the use of "Honey-pots" where fake or dummy assets are created and exposed to attackers for the purpose of learning attack signatures and attack behaviors for use in protecting "Real" critical assets. **Barriers:** Cyber protection, detection and recovery technologies will always evolve. The organization may decide when, and at what CAPEX amount should they upgrade their systems and technologies to improve their cyber defenses. The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**Operational Requirement(s):** Organizations may share what they learn about Threats, Attacks, Signatures, and remediation/recovery information with trusted organizations, government entities and trusted industry peers. * Organizations can maintain maximum operational security and never divulge critical details of their cyber protection, and recovery procedures and technologies in public fora.	· **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4

			Technology Requirement(s): The utilization of secure communication and encryption is vital to the sharing of cyber protection technologies, methods and procedures. **Barriers:** **Existing laws and regulations may limit the ability to share threat information.** Trusted entities may not be receptive to the sharing of cyber protection related information. Trusted entities may not reciprocate the sharing of cyber protection related information.	
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**Operational Requirement(s):** * Organizations may develop/document a formalized Incident Response Plan. This Incident Response Plan should contain, but not limited to the following areas: Preparation / Incident Identification / Incident Containment / Incident-Threat Eradication / Recovery / and Lessons Learned. This Incident Response Plan may be approved by the highest levels of organizational leadership and by all data/system/network owning business units. * Organizations may develop/document a formalized Business Continuity(BC)/Disaster Recovery(DR) Plan. This Business Continuity/Disaster Recovery Plan may contain, but not limited to the following areas: / Equipment failures / Disruption of power and telecommunications / Application failure or corruption of databases / Human error, sabotage / Malicious Software (Viruses, Worms, Trojan horses) attack / Hacking-Internet attacks / terrorist attacks / Fire / Natural disasters (Flood, Earthquake, Hurricanes), BC/DR Response Team(s) / Responsibilities of BC/DR Response Team(s) / BC/DR Communications / Business Recovery procedures / and Lessons Learned. This Business Continuity/Disaster Recovery Plan may be approved by the highest levels of organizational leadership and by all data/system/network owning business units. **Technology Requirement(s):**	· **COBIT 5** DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 · **NIST SP 800-53 Rev. 4** CP-2, IR-8

			The organization may consider DR technologies, systems, protocols, networks, off-site data storage facilities, and services. There may be more than adequate storage capacity, database capacity, and network bandwidth to allow frequent backups of critical information and data. * Organizations may wish to consider implementing complete full-scale disaster recovery technologies. **Barriers:** There will be an additional CAPEX cost to procuring DR technologies and off-site services like storage and data recovery. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Business Continuity and Disaster Recovery	
		PR.IP-10: Response and recovery plans are tested	**Operational Requirement(s):** * Organizations may TEST formalized Incident Response Plans on a regular and frequent basis. This Incident Response TESTING can contain, but not limited to the following areas: Preparation / Incident Identification / Incident Containment / Incident-Threat Eradication / Recovery / and Lessons Learned. This Incident Response TESTING may be coordinated with all levels of organizational leadership and by all data/system/network owning business units. * Organizations may TEST formalized Business Continuity(BC)/Disaster Recovery(DR) Plans on a regular and frequent basis. This Business Continuity/Disaster Recovery TESTING may contain, but not limited to the following areas: BC/DR Response Team(s) Responsibilities / BC/DR Communications / Business Recovery procedures / and Lessons Learned. This Business Continuity/Disaster Recovery TESTING may be coordinated with levels of organizational leadership and by all data/system/network owning business units. **Technology Requirement(s):** The organization may consider DR technologies, systems, protocols, networks, off-site data storage facilities, and services. There may be more than adequate storage capacity, database capacity, and network bandwidth to allow frequent backups of critical information and data. * Organizations may wish to consider implementing complete full-scale disaster recovery technologies.	· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14

			Barriers: There will be an additional CAPEX cost to procuring DR technologies and off-site services like storage and data recovery. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Business Continuity and Disaster Recovery	
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**Operational Requirement(s):** Organizations, sub-organizations and all data owners who manage and maintain information technology assets may receive comprehensive training on implementing cybersecurity best practices. * Organizations may disable / decommision / wipe / destroy all account privileges for employees that have departed the organization. * Organizations may develop and implement a Mobile Device management and Security Plan-Policy. This plan may include but not limited to: Authorized access control / VPN Access control / Encryption control / Authorized system connections / Mobile Device Threats / Mobile Device Security testing / Mobile device patching and update frequency / Loss of Device procedures / Employee termination procedures / Employee mobile device responsibilities & rights. * Organizations may deploy ENDPOINT device continuous monitoring and security management functions. ENDPOINTs include but not limited to computers / servers / VMs / tablets / smartphones / storage devices / hubs / any devices that connects to the public Internet and external (Cloud) data centers. **Technology Requirement(s):** An organization's IT department, may have to procure mobile and Endpoint device management technologies that will also disable / decommission / wipe / destroy all account privileges for employees that have departed the organization. **Barriers:** There will be an additional CAPEX cost to procuring Endpoint and Mobile Device management technologies. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Endpoint and Mobile Device management.	· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS Family

		PR.IP-12: A vulnerability management plan is developed and implemented	**Operational Requirement(s):** Organizations may establish and document a Threats/Vulnerabilities management plan as it relates to critical infrastructure * Organizations may identify ~~all~~ possible threats and vulnerabilities to their critical infrastructure assets, including, but not limited to: Unauthorized Access / Data Breaches / Malware / DDoS / Advanced Persistent Threats / Zero-day Attacks / Phishing / SQL Injections / USB injected bots / and False alarms. * Organizations may conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. * Organizations may consider executing penetration testing and vulnerability scanning exercises on a weekly basis. * Organizations should consider the use of "Sandboxing" or the use of "Honey-pots" where fake or dummy assets are created and exposed to attackers for the purpose of learning attack signatures and attack behaviors for use in protecting "Real" critical assets. * Organizations may strive to REDUCE Their attack surface. The attack surface can be reduced by executing the following: Reduce the number of open ports and services on Internet-facing systems / Eliminate all unnecessary protocols and services from endpoints, servers and internal systems / Implement a least-privilege access control policy / Deploy Next Gen Firewalls to control access to applications and network resources. **Technology Requirement(s):** None **Barriers:** The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance	**PR.MA-1:**	**Operational Requirement(s):**	· **COBIT 5**

	(PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Organizations may monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations can classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may collect data and track all activities with critical assets. This may include, but not limited to logging of all logins, applications used, files accessed/copied/downloaded, all doors opened, Internet connections/URLs / times these events occurred and who conducted these activities. **Technology Requirement(s):** Access control / logging / disabling technologies and systems may have to be deployed to protect critical assets. **Barriers:** There will be an additional CAPEX cost to procuring Access control / logging / disabling technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Access control / logging / disabling technologies and systems.	BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**Operational Requirement(s):** Organizations may monitor and control critical infrastructure asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * Organizations can classify, compartmentalize and segment their critical assets and data. Establish "Zones" of various levels of trust, including a "Zero-Trust" Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network.	· **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1

			* Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may collect data and track all activities with critical assets. This may include, but not limited to logging of all logins, applications used, files accessed/copied/downloaded, all doors opened, Internet connections/URLs / times these events occurred and who conducted these activities. **Technology Requirement(s):** Access control / logging / disabling technologies and systems may have to be deployed to protect critical assets. **Barriers:** There will be an additional CAPEX cost to procuring Access control / logging / disabling technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Access control / logging / disabling technologies and systems.	· **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**Operational Requirement(s):** Organizations may collect data and track all activities with critical infrastructure assets. This may include, but not limited to logging of all logins, applications used, files accessed/copied/downloaded, all doors opened, Internet connections/URLs / times these events occurred and who conducted these activities. **Technology Requirement(s):** Access control / logging / disabling technologies and systems may have to be deployed to protect critical assets. **Barriers:** There will be an additional CAPEX cost to procuring Access control / logging / disabling technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be	· **CCS CSC** 14 · **COBIT 5** APO11.04 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1

			responsible for Access control / logging / disabling technologies and systems.	· **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	**Operational Requirement(s):** Organizations may identify ~~all~~ possible threats and vulnerabilities to their infrastructure assets, including, but not limited to: Unauthorized Access / Data Breaches / Malware / DDoS / Advanced Persistent Threats / Zero-day Attacks / Phishing / SQL Injections / USB injected bots / and False alarms. * Organizations may deploy ENDPOINT device continuous monitoring and security management functions. ENDPOINTs include but not limited to computers / servers / VMs / tablets / smartphones / storage devices / USB drives-devices / Bluetooth devices / hubs / any devices that connects to the public Internet and external (Cloud) data centers. **Technology Requirement(s):** USB drives, Bluetooth devices and any wireless device that can store information, should be tracked / inventoried / disposed of properly if they are allowed in an organization's operational environment. **Barriers:** Staff may use these devices (often personal devices), regardless of organization's policy on removable media usage.	· **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to	**Operational Requirement(s):**	· **COBIT 5**

		systems and assets is controlled, incorporating the principle of least functionality	* The organization can determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization may take into account "all" internal communications with: Tiers I,II,III of critical infrastructure related operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. * The organization may set access controls-business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * Organization may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. * The Organization can implement an Access-Permission policy based on ***Separation of duties*** and ***Least Privilege***. Separation of duties requires dividing all organizational functions among multiple people to limit the possibility that one employee could harm an organization without the cooperation of others. * The separation of duties policy also requires implementation of least privilege, which means authorizing people to use only the resources needed to do their job. * Organizations can manage least privilege as an ongoing process, particularly when employees move through the organization as a result of promotions, transfers, relocations, demotions, and especially terminations. Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber-attack. * The organization may carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove permissions that are no longer needed. The organization may establish account management policies and procedures and regularly audit account activity. * Once these access-permission policies and procedures are established, all personnel can be trained and continuously reminded of their roles, responsibilities and any enforceable actions that can occur, should there be any intentional violations.* Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations can monitor and control critical asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data.	DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7

			Technology Requirement(s): Access control / logging / disabling technologies and systems may have to be deployed to protect critical assets. **Barriers:** *There may be personnel internal and external to the organization (staff, suppliers, customers, partners) that believe that their credentials have been wrongfully applied. The organization should develop business and cybersecurity rules that determine who is authorized to do what within the organization's infrastructure. If there are still disagreements and conflicts, then an organization's leadership and management should decide on a case-by-case basis. There will be an additional CAPEX cost to procuring Access control / logging / disabling technologies and systems. * There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Access control / logging / disabling technologies and systems.	
		PR.PT-4: Communications and control networks are protected	**Operational Requirement(s):** Organizations may protect critical infrastructure related physical and virtual circuits, networks and communications systems from attack and DDoS by employing Next-Gen firewalls, session border controllers (SBC), IPv6, encryption technologies and the latest cyber/network security best practices. * Organizations can stay abreast of the latest types of attacks against communications protocols and employ best practices and practical technologies to protect critical communications. **Technology Requirement(s):** Organizations may have to procure and deploy Next-Gen Firewalls, Session border controller(SBC), software-application firewalls and encryption technologies in order to protect critical communications. **Barriers:** There will be an additional CAPEX cost to procuring Firewall, SBC, encryption technologies and systems.	· **CCS CSC** 7 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7

			There will be an additional OPEX cost to allocate, hire, train staff to be responsible for the operations of Firewall, SBC, encryption technologies and systems.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	**Operational Requirement(s):** The organization and appropriate staff can develop, document, and maintain under configuration control, a current baseline configuration of the critical infrastructure information system. Baseline configurations include information about information system components (e.g. standard software packages installed on workstastions, notebook computers, servers, network components, or mobile devices) along with the network topology. The organization may maintain baseline configurations by creating new baselines as organizational informational systems change over time. * The organization may determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization should take into account "all" internal communications with: Tiers I,II,III of operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. Once these communication paths and flows have been determined the organization may set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. The entire flow of information that describes who-what-when-how can be documented and conveyed through ongoing training, to the effected personnel. **Technical Requirements:** The organization may employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. Mechanisms can include hardware and software inventory tools, configuration management tools, and network management tools. These tools, for example, can be used to track version numbers of software. **Barriers:** *The Operational requirements to map an organization's communications flow will require assigning and allocating staff (that may be assigned to other functions), to document this flow and to keep it updated with business and	· **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4

			personnel changes.	
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**Operational Requirement(s):** The organization and appropriate staff can correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response for critical infrastructure. The organization may also employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organization processes for investigation and response to suspicious activities. The organization then may analyze and correlate audit records across different repositories to gain organization-wide situational awareness. * Organizations should conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. * Organizations may decide whether to respond immediately to an incident, which may cause an attacker to wipe malicious code, files and toolsets from compromised systems –or- to monitor the attacker's activity in order to gain further threat intelligence to prevent future attacks. * Organizations may share and learn Threat, Attack, Signature, and remediation information with and from trusted organizations, government entities and trusted peers. **Technical Requirements:** Organizations may consider automated mechanisms for centralized and analysis includes, for example, Security Information Management(SIEM) technologies. * Organizations may consider the use of "Sandboxing" or the use of "Honey-pots" where fake or dummy assets are created and exposed to attackers for the purpose of learning attack signatures and attack behaviors for use in protecting "Real" critical assets. **Barriers:** The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack. There will be an additional CAPEX cost to procure detection and analysis tools and technologies.	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data	**Operational Requirement(s):**	· **ISA 62443-3-**

		are aggregated and correlated from multiple sources and sensors	The organization and appropriate staff can properly track and document information system security incidents for critical infrastructure. This can include an automated mechanism to assist in the tracking of security incidents and the collection and analysis of incident information. Also, the organization and appropriate staff may develop an incident response plan that defines the resources and management support needed to effectively maintain and mature your incident response capabilities. * Organizations can monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations can implement 'Continuous' network, system, data, and storage information collection, and alert upon deviations from normal BASELINE asset behavior. * Organizations can conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. **Technical Requirements:** Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers or other electronic databases of incident handling. **Barriers:** *Professional staff may be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust may need to be established and additional levels of training should take place. * The chosen sources to which threats and vulnerabilities can be drawn from, may violate the organization cybersecurity policies and procedures. * The organization can use extreme caution and ensure that these sources do not connect directly to critical networks and systems. They can be used as information sources only. * There will be an additional CAPEX cost to procure detection and analysis tools and technologies.	**3:2013** SR 6 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of	**Operational Requirement(s):**	· **COBIT 5**

		events is determined	The organization and appropriate staff can coordinate with external organizations to correlate and share incident information to achieve a cross-organization perspective of the security event as it relates to critical infrastructure. * The organization may also employ automatic tools to support near real-time analysis of events. * The organization may also identify critical information system assets and the resources in which they support. * Organizations may identify ~~all~~ possible threats and vulnerabilities to their assets, including, but not limited to: Unauthorized Access / Data Breaches / Malware / DDoS / Advanced Persistent Threats / Zero-day Attacks / Phishing / SQL Injections / USB injected bots / and False alarms. * Organization may determine the consequences of various cyber incidents. These consequences may include, but not limited to degradation of public trust / financial and market losses / degradation of brand reputation / impact to critical infrastructure. **Technical Requirements:** Automatic tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems. * Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents. These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking / Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. **Barriers:** *Professional staff should be allocated/assigned to this task, which may cause an increase in salaries, benefits, administration and logistics OPEX costs. Additional levels of trust can be established and additional levels of training can take place.	APO12.06 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4

		DE.AE-5: Incident alert thresholds are established	**Operational Requirement(s):** When organizations employ monitoring, scanning and collection functions, and baselines have been set for 'normal' behavior, the organization may establish thresholds of incident alerts, where valid problems are alerted upon, and keeps false alarms to a minimum. This can be an iterative process and the thresholds should be adjusted as the organization learns more details of 'normal' behavior as it relates to critical infrastructure. **Technical Requirements:** Systems for monitoring, scanning and collection will need their parameters adjusted as thresholds are established and changed. **Barriers:**	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.2.3.10 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**Operational Requirement(s):** The organization and appropriate staff monitors the information system to detect attacks and indicators of potential attacks in accordance with defined monitoring objectives for critical infrastructure. The organization may be looking for unauthorized local, network, and remote connections. To accomplish this organization may deploy monitoring devices strategically within the information system to collect organization-determined essential information, and at ad hoc locations within the system to track specific types of transactions of interests to the organization. * Organizations may continuously monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations may consider executing penetration testing and vulnerability scanning exercises on a weekly basis. **Technical Requirements:**	· **CCS CSC** 14, 16 · **COBIT 5** DSS05.07 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

			The organization may employ different monitoring tools, e.g., host monitoring, network monitoring, and anti-virus software. * Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents. These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking / Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. **Barriers:** The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**Operational Requirement(s):** For critical infrastructure, the organization and appropriate staff may establish procedures for monitoring and alarming when physical or environmental security is compromised. * Physical and environmental security measures can be designed to complement the cyber security measures taken to protect assets that are part of the information system. When developing a program for physical security of assets, it is important to include all systems in the scope and not just limit the effort to traditional computer room facilities. * Organizations can monitor and control critical asset configuration and installation changes. Only authorized staff and departments may be allowed to change the physical and virtual configurations of critical assets, software, applications, databases and stored data. * The organization may determine whom within, internal and external to the entire organization, may be allowed "PHYSICAL" access to critical networks systems, computing systems, storage systems, databases, email systems, technical spaces, data centers, wiring closets, servers rooms, devices, tools, vehicles etc. that allow the organization to be an on-going concern. These critical systems may be protected from unauthorized 'physical' access by locked doors, locked equipment cabinets, locked file and	· **ISA 62443-2-1:2009** 4.3.3.3.8

			software cabinets, locked fencing, biometric locks to shared technical areas, locked vehicles, locked property and even building/landscaping designs to prevent brute-force entries to critical areas. **Technical Requirements:** Physical segmentation is a key security countermeasure designed to compartmentalize devices into security zones where identified security practices are employed to achieve the desired target security level. * The entire physical protection environment for critical infrastructure should be monitored and managed by an automated, easy to use system that can see and detect entry by authorized and unauthorized persons. This automated physical protection management system can also have the integrated ability to allow authorized operations personnel (i.e.; a NOC) to visibly see critical/protected assets, collect/store/playback video of protected assets, lock and unlock physical assets, doors, entry ways, vehicles etc., remotely. **Barriers:** * There will be CAPEX and OPEX costs associated with procuring, installing and managing a physical protection management system. There will be a time element associated with evaluating systems, vendors and their abilities to deliver a physical protection management system. There will be a time element to the implementation, testing, acceptance and training associated with a new physical protection management system.	
		DE.CM-3: Personnel	**Operational Requirement(s):**	· **ISA 62443-3-**

		activity is monitored to detect potential cybersecurity events	The organization and appropriate staff may identify and select the proper types of critical infrastructure information, system accounts to support, i.e. administrator, user, etc. The organization can then assign account managers for the system information accounts, establish account privileges, and monitor the use of information system accounts, including deleting accounts promptly and when necessary. * Organizations may collect data and track all activities with critical assets. This may include, but not limited to logging of all logins, applications used, files accessed/copied/downloaded, all doors opened, Internet connections/URLs / times these events occurred and who conducted these activities. * Access control based on separation of duties and least privilege is crucial to mitigating the threat of an insider cyber-attack. * The organization can carefully audit user access permissions when an employee changes roles in the organization to avoid insider vulnerabilities and threats. In addition, audit user access permissions frequently, to remove permissions that are no longer needed. **Technical Requirements:** Access control / logging / disabling technologies and systems may have to be deployed to protect critical infrastructure assets. * The organization may employ an information system that automatically can remove temporary and emergency account after a designated time period. This system may also disable inactive account after a certain amount of time. In addition, the system can be configured to log out inactive users after a defined time-period. * Access control / logging / disabling technologies and systems may have to be deployed to protect critical assets. **Barriers:** There will be an additional CAPEX cost to procuring Access control / logging / disabling technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Access control / logging / disabling technologies and systems.	**3:2013** SR · **ISO/IEC 27001:2013** A.12.4.1 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious	**Operational Requirement(s):**	· **CCS CSC** 5

		code is detected	For critical infrastructure, the organization and appropriate staff employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. * The organization may configure the malicious code protection to perform periodic scans of the information system at a defined frequency and real-time scans of files from external sources at the network endpoints. This program may be configured to block or quarantine malicious code and send alert to all administrators. **Technical Requirements:** The organization may implement nonsignature-based malicious code detection mechanisms, which include the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. **Barriers:** There will be an additional CAPEX cost to procuring malicious code protection and detection technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for malicious code protection and detection technologies and systems.	· **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: Unauthorized mobile code is detected	**Operational Requirement(s):** For critical infrastructure, the organization and appropriate staff may define acceptable and unacceptable mobile code and mobile code technologies. * The organization also can establish usage restrictions and implementations guidance for acceptable mobile code and mobile code technologies. * The organization may authorize, monitor, and control the use of mobile code within the information system as it relates to critical infrastructure. * Organizations may develop and implement a Mobile Device management and Security Plan-Policy. This plan may include but not limited to: Authorized access control / VPN Access control / Encryption control / Authorized Apps & mobile software / Authorized system connections / Mobile Device Threats / Mobile Device Security testing / Mobile device patching and update frequency / Loss of Device procedures / Employee termination procedures / Employee mobile device responsibilities & rights.	· **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1 · **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44

			Technical Requirements: The organization may implement nonsignature-based malicious code detection mechanisms, which include the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. * The organization may consider deploying Mobile Device Management(MDM) technologies. These MDM systems may employ an information system which prevents the automatic execution of mobile code in certain software applications and enforces actions to be carried out prior to executing the code. Actions before executing the code, may include, prompting users prior to opening electronic mail attachments. Preventing automatic execution of code may include disabling auto execute features on information system components employing portable storage devices. **Barriers:** There will be an additional CAPEX cost to procuring malicious code protection and detection technologies and MDM technologies. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for malicious code protection and detection and MDM technologies.	
		DE.CM-6: External	**Operational Requirement(s):**	· **COBIT 5**

		service provider activity is monitored to detect potential cybersecurity events	For critical infrastructure, organizations may require that service providers of external information system services comply with organizational information security requirements and employ mechanisms to monitor compliance by external providers on an ongoing basis. * Organizations can monitor and control critical asset configuration and installation changes. * Organizations can classify, compartmentalize and segment their critical assets and data. Establish “Zones” of various levels of trust, including a “Zero-Trust” Zone for the most critical data and network assets. Zero-Trust Zones mean no default trust is allowed for any entity, user, device, application, or packet regardless of what it is and its location in the network. * Organizations may only allow granular control of devices, data, content, network access and applications to only authorized users and authorized sub-organizations. * Organizations may collect data and track all activities with critical assets. This may include, but not limited to logging of all logins, applications used, files accessed/copied/downloaded, all doors opened, Internet connections/URLs / times these events occurred and who conducted these activities. * The organization may determine whom within, internal and external to the entire organization, should be allowed "REMOTE" access to critical networks systems, computing systems, storage systems, databases, email systems, technical spaces, data centers, wiring closets, servers rooms, devices, tools, vehicles etc. that allow the organization to be an on-going concern. These critical systems may be protected from unauthorized 'REMOTE' access by mechanisms including, but not limited to: firewalls, USERNAME/PASSWORDs, multi-factor identification, access control lists, scheduling limits, VPN access, LAN/WAN access, biometrics, encryption keys etc. * Organizations can monitor physical and virtual circuits and networks connecting to service providers for fraudulent and malicious activities within the native protocols that serve these circuits. **Technical Requirements:** Access control / logging / disabling technologies and systems may have to be deployed to protect critical infrastructure assets. * The organization may employ an information system that automatically can remove temporary and emergency account after a designated time period. This system may also disable inactive account after a certain amount of time. In addition, the system can be configured to log out inactive users after a defined time-period. * Session border controllers, firewalls and analytics may need to	APO07.06 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4

			be deployed to detect anomalies from connected service providers. **Barriers:** There will be an additional CAPEX cost to procuring Access control, SBC and Firewall technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Access control, SBC and Firewall technologies and systems.	
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**Operational Requirement(s):** For critical infrastructure, the organization and appropriate staff may develop a monitoring strategy and implement a continuous monitoring program, which includes organization metrics to be monitored and the frequency at which to monitor these metrics. The organization can analyze and assess the information that is generated by this monitoring program for any anomalies or security concerns. * Organizations may monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. **Technical Requirements:** The organization may deploy automated monitoring tools to help in its monitoring efforts for critical infrastructure. Automated tools include, for example, host-based, network-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizations information systems. * Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents. These tools and technologies should include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking /	· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4

			Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. **Barriers:** There will be an additional CAPEX cost to procuring SIEM technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for SIEM technologies and systems.	
		DE.CM-8: Vulnerability scans are performed	**Operational Requirement(s):** For critical infrastructure, the organization and appropriate staff can scan for vulnerabilities in the information system and hosted applications at a defined frequency and when new vulnerabilities potentially affecting the system/applications are identified and reported. The process may include analyzing the scans and correcting legitimate vulnerabilities. * Organizations may consider executing penetration testing and vulnerability scanning exercises on a weekly basis. **Technical Requirements:** The organization may implement vulnerability scanning tools that include the capability to readily update the information systems vulnerabilities to be scanned. Also, automated mechanisms to compare the results of vulnerability scans over time may be implemented to determine trends. **Barriers:** There will be an additional CAPEX cost to procuring scanning & data collection technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for scanning & data collection technologies and systems.	· **COBIT 5** BAI03.10 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**Operational Requirement(s):** The organization and appropriate staff develops a security assessment plan that describes the scope of the assessment, including employing assessors or assessment teams with a level of independence to conduct security control assessments of critical infrastructure assets. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interests with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organization they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. * Organizational leadership, operations and engineering staff should determine who (by job function) has various levels of cybersecurity responsibilities and leadership should be assigned. These levels of cybersecurity responsibilities will include but not limited to: Detection / Incident Response / BC-DR / Security of entire infrastructure / security of groups of systems - applications - databseses/SW/devices, security of individual systems/applications/databseses/SW/devices, as well as security of internal and external communications channels. The cybersecurity leadership can then develop cybersecurity policies and procedures, then train the appropriate staff of these cybersecurity procedures. * Organizations, sub-organizations and all data owners who manage and maintain information technology assets may receive comprehensive training on implementing cybersecurity best practices. * Organizations may consider various types of resources for responding to cyber incidents. These resources include, but not limited to: Incident Response Team pulled from existing staff as incident arise / Response Team of staff dedicated to incident response, reporting, remediation / Third-party response services and providers. **Technical Requirements:** Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents. These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access	· **CCS CSC** 5 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14

			control / SSL Decryption / Log analysis / File-content filtering-blocking / Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. **Barriers:** There will be an additional CAPEX cost to procuring SIEM / IPS / IDS technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for SIEM / IPS / IDS technologies and systems.	
		DE.DP-2: Detection activities comply with all applicable requirements	**Operational Requirement(s):** For critical infrastructure, the organization and appropriate staff should develop a plan to monitor the information systems and technical assets of an organization and obtain legal opinion with regards to the monitoring activities to ensure these activities are in accordance with applicable federal laws, privacy considerations, Executive Orders, directives, policies, or regulations. **Technical Requirements:** None **Barriers:** Some techniques, methods and technologies may cross legal and regulatory boundaries, and legal and regulatory requirements may vary across sectors.	· **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	**Operational Requirement(s):** The organization and appropriate staff may test critical infrastructure intrusion-monitoring tools at a defined frequency. Testing intrusion-monitoring is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of the organization. * Organizations may consider executing penetration testing and vulnerability scanning exercises on a periodic basis (e.g. weekly).	· **COBIT 5** APO13.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC**

			Technical Requirements: Organizations can procure Cyber Incident Detection tools and technologies that can be adequately tested without disabling live-operational systems and networks. **Barriers:** In order to make testing as realistic as possible, some detection methods and technologies may have a negative impact on live-operational systems and networks. The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	**27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	**Operational Requirement(s):** The organization and appropriate staff may share information obtained from the vulnerability scanning process and security control assessments with appropriate staff to help eliminate similar vulnerabilities in other critical infrastructure information systems. This could include automatic alerts from the information system itself that conveys the information to the appropriate staff. * Organizations can monitor and establish BASELINE network traffic, file access, database activity, software modifications, stored data access, and overall assets behavior, in order to better detect anomalies, unauthorized access, breaches and attacks. * Organizations can conduct frequent correlation of threat detection intelligence with live collected network, system, data, and storage information. * Organizations may share and learn Threat, Attack, Signature, and remediation information with and from trusted organizations, government entities and trusted peers. **Technical Requirements:** For critical infrastructure the organization may deploy an information system that alerts appropriate personnel when there is an indication that a compromise has or may occur. Alerts may be generated from a variety of sources, including, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4

			Barriers: There will be an additional CAPEX cost to procuring SIEM / IPS / IDS technologies and systems. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for SIEM / IPS / IDS technologies and systems.	
		DE.DP-5: Detection processes are continuously improved	**Operational Requirement(s):** The organization and appropriate staff may analyze communication traffic/event patterns for the critical infrastructure information system; develop profiles representing common traffic patterns and/or events; and use the traffic/event profiles for tuning system-monitoring devices to reduce the number of false positives and the number of false negatives. In addition, the organization may use trend analysis to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in continuous monitoring process need to be modified based on empirical data. * Organizations may consider the use of "Sandboxing" or the use of "Honey-pots" where fake or dummy assets are created and exposed to attackers for the purpose of learning attack signatures and attack behaviors for use in protecting "Real" critical assets. * Organizations can strive to identify a cyber incident as rapidly as possible and reach incident containment within 1 to 4 hours. * Organizations can track and measure performance times and seeks ways to reduce time to containment. * Organizations can catalog lessons learned from every cyber incident. These lessons learned catalog should include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:** Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents. These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking /	· **COBIT 5** APO11.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

			Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. **Barriers:** There will be an additional CAPEX and OPEX cost to procuring SIEM / IPS / IDS technologies and systems and training staff. The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	**Operational Requirement(s):** The organization and appropriate staff may provide the capability to restore critical infrastructure information system components within a specified time to a known operational state of the system. The organization and appropriate staff may also identify classes of incidents and the appropriate responses to these incidents to ensure a response plan can be carefully carried out. * Organizations can strive to identify a cyber incident as rapidly as possible and reach incident containment within 1 to 4 hours. Organizations should track and measure performance times and seeks ways to reduce time to containment. * Organizations can strive to identify a cyber incident as rapidly as possible and achieve full business recovery and remediation within 1 to 24 hours. Organizations can track and measure performance times and seeks ways to reduce time to Recovery. * Organizations can catalog lessons learned from every cyber incident. These lessons learned catalog should include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:**	· **COBIT 5** BAI01.10 · **CCS CSC** 18 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8

			Before and during execution of the response plan, the organization can use fall back technologies that allows information systems to operate in a reserved mode while being reconfigured. * The organization may consider DR technologies, systems, protocols, networks, off-site data storage facilities, and services. There may be more than adequate storage capacity, database capacity, and network bandwidth to allow frequent backups of critical information and data. * Organizations may wish to consider implementing complete full-scale disaster recovery technologies. **Barriers:** Lack of staff dedicated to Incident Response will hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / specialized technologies will hinder an effective response to an attack, breach or loss of data. * Lack of formal, and Ad-Hoc communications between sub-organizations, suppliers, and service providers before, during and in response to a cyber incident, will hinder any effective incident response. There will be an 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.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**Operational Requirement(s):** The organization and supporting staff may develop an incident response plan that provides a roadmap for implementing its incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; and defines reportable incidents etc. This plan may be provided to organization-defined incident response personnel as it relates to critical infrastructure. * Organizations may develop/document a formalized Incident Response Plan. This Incident Response Plan may contain, but not limited to the following areas: Preparation / Incident Identification / Incident Containment / Incident-Threat Eradication / Recovery / and Lessons Learned. This Incident Response Plan may be approved by the highest levels of organizational leadership and by all data/system/network owning business units. **Technical Requirements:**	· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8

			The organizations can ensure that secure, reliable electronic communications (email, text, voice comms., etc.) are in place, so that appropriate personnel are alerted into action when an incident response is required. **Barriers:** Lack of staff dedicated to Incident Response will hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / specialized technologies will hinder an effective response to an attack, breach or loss of data. * Lack of formal, and Ad-Hoc communications between sub-organizations, suppliers, and service providers before, during and in response to a cyber incident, will hinder any effective incident response.	
		RS.CO-2: Events are reported consistent with established criteria	**Operational Requirement(s):** The organization and appropriate staff require the reporting of suspect security incidents within a specified time to the appropriate personnel. The organization then may provide security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident. * Organizational leadership, operations and engineering staff can determine who (by job function) needs to know what information within the entire organization. Following this exercise, various levels of cybersecurity responsibilities and leadership should be assigned. The cybersecurity leadership may then develop cybersecurity policies and procedures, then train the appropriate staff of these cybersecurity procedures. * Once the information security policies are established within an organization, these policies may be conveyed to the appropriate levels of executives, management, and staffing, such that everyone knows their responsibilities in protecting various types of information. External policies and procedures for protecting information, may also be developed. These externally facing information security policies and procedures may also be strongly conveyed to external suppliers, partners, peers and 3rd party entities that support the organization. * Organizations, sub-organizations and all data owners who manage and maintain information technology assets may receive comprehensive training on implementing cybersecurity best practices.	· **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8

			Technical Requirements: The organizations can ensure that secure, reliable electronic communications (email, text, voice comms., etc.) are in place, so that appropriate personnel are alerted into action when an incident response is required. **Barriers:** There may be an additional OPEX cost of hiring specialized personnel and/or assigning cybersecurity responsibilities to staff. These cybersecurity responsibilities, policies and procedures will constantly need updating to keep pace with business changes, evolving security climates and personnel changes.	
		RS.CO-3: Information is shared consistent with response plans	**Operational Requirement(s):** The organization and appropriate staff may incorporate into their critical infrastructure information system monitoring mechanism, automatic means to alert security personnel of inappropriate or unusual activities with security implications. * The organization deploys near real time analysis of events and anomalies that occur within the information system. This analysis may not only include information involving direct attacks but also information regarding potential threats as well. * Organizations may share and learn Threat, Attack, Signature, and remediation information with and from trusted organizations, government entities and trusted peers. **Technical Requirements:** The organizations can ensure that secure, reliable electronic communications (email, text, voice comms., etc.) are in place, so that appropriate personnel are alerted into action when an incident response is required. **Barriers:** There may be an additional OPEX cost of hiring specialized personnel and/or assigning cybersecurity responsibilities to staff. These cybersecurity responsibilities, policies and procedures will constantly need updating to keep pace with business changes, evolving security climates and personnel	· **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4

			changes.	
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**Operational Requirement(s):** The organization and appropriate staff may coordinate its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied. * Organizations may share and learn Threat, Attack, Signature, and remediation information with and from trusted organizations, government entities and trusted peers. * The organization can determine "who-externally" needs to know "what" information, "when" and "how" will that information be delivered. The organization may take into account "all" external communications with: vendors/suppliers, emergency responders, government officials, peers, customers, public facing websites, customer portals, contact centers, legal entities, , service providers, executive communications, billing interfaces, eCommerce interfaces, mobile/remote employees etc. * Once these communication paths and flows have been determined the organization should set access controls- business process rules within various systems to allow authorized personnel to reach their required information, when they need it to perform their job function. The entire flow of information that describes who-what-when-how should be documented and conveyed through ongoing training, to the effected personnel. * Organizations may develop a policy for connecting to external information systems and prohibit, where necessary, the direct connection to a public network. Organization can develop a baseline security compliance policy for all external components connecting to the information system (e.g. mobile phones, printers, laptops, etc.) **Technical Requirements:** The organizations can ensure that secure, reliable electronic EXTERNAL communications (email, text, voice comms., etc.) are in place, so that appropriate 3rd parties/Stakeholders/ 1st Responder personnel are alerted into action when an incident response is required. **Barriers:**	· **ISA 62443-2-1:2009** 4.3.4.5.5 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

			There may be an additional OPEX and CAPEX costs associated with back-up/redundant services from service providers and trusted 3rd parties who may be needed in response to an incident. Lack of formal, and Ad-Hoc communications between sub-organizations, suppliers, and service providers before, during and in response to a cyber incident, will hinder any effective incident response.	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**Operational Requirement(s):** The organization and appropriate staff establish and institutionalize contact with selected groups and associations within the security community. The organization may then develop a channel to receive information system security alerts, advisories, and directives from these organizations on an ongoing basis. * Organizations may share and learn Threat, Attack, Signature, and remediation information with and from trusted organizations, government entities and trusted peers. **Technical Requirements:** The organization can employ automated mechanisms to make security alert and advisory information available throughout the organization. * Organizations may ensure that secure, reliable electronic EXTERNAL communications (email, text, voice comms....., etc.) are in place, so that appropriate 3rd parties/Stakeholders/ 1st Responder personnel are alerted into action when an incident response is required. **Barriers:** There may be an additional OPEX and CAPEX costs associated with back-up/redundant services from service providers and trusted 3rd parties who may be needed in response to an incident. Lack of formal, and Ad-Hoc communications between sub-organizations, suppliers, and service providers before, during and in response to a cyber incident, will hinder any effective incident response. The lack of legislative clarity regarding cyber threat information sharing may also hinder incident response.	· **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN):	**RS.AN-1:**	**Operational Requirement(s):**	· **COBIT 5**

	Analysis is conducted to ensure adequate response and support recovery activities.	Notifications from detection systems are investigated	The organization and appropriate staff may review and analyzes critical infrastructure information system audit records at specified intervals for indications of unauthorized activities. The anomalies can be reported to the appropriate staff. * The information system provides the capability to centrally review and analyze audit records from multiple components within the system. Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. * Organizations may conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. * Organizations can strive to identify a cyber incident as rapidly as possible and reach incident containment within 1 to 4 hours. * Organizations should track and measure performance times and seek ways to reduce time to containment. * Organizations may decide whether to respond immediately to an incident, which may cause an attacker to wipe malicious code, files and toolsets from compromised systems –or- to monitor the attacker's activity in order to gain further threat intelligence to prevent future attacks. * Organizations may conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. * Organizations can be vigilant against Advance Persistent Threats (APTs) by constantly monitoring for Attacker reconnaissance / Attacker incursion / Attacker response if discovered / Attacker capture of systems / Attacker outbound communications and stolen data transfer. **Technical Requirements:** Organizations may consider deploying various tools and technologies to PREVENT / MITIGATE / RESPOND and RECOVER from cyber-attack incidents. These tools and technologies may include, but not limited to: Network port scanning / packet capture-inspection / Intrusion Detection-Protection(IPS/IDS) / Endpoint monitoring-security / Threat correlation functions / Digital forensics / Data-File flow and anomaly detection / Access control / SSL Decryption / Log analysis / File-content filtering-blocking / Outbound botnet communication disruption / Secure Email gateways / Big-data security analytics / and Next Gen Firewalls. * Organizations may deploy ENDPOINT device continuous monitoring and security management functions. ENDPOINTs include but not limited to computers / servers / VMs / tablets / smartphones / storage devices / hubs / any devices that connects to the public Internet and external (Cloud) data centers. * Organizations can	DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

			be vigilant against Advance Persistent Threats (APTs) by implementing tools that constantly monitor for Attacker reconnaissance / Attacker incursion / Attacker response if discovered / Attacker capture of systems / Attacker outbound communications and stolen data transfer. **Barriers:** False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to investigate the detection of cyber incidents.	
		RS.AN-2: The impact of the incident is understood	**Operational Requirement(s):** Organization can determine the consequences of various cyber incidents as it relates to critical infrastructure. These consequences may include, but not limited to impact to supply chain / degradation of public trust / financial and market losses / degradation of brand reputation / impact to critical infrastructure. * The organization and appropriate staff correlates incident information and individual incident response to achieve an organization-wide perspective on incident awareness and response. * The organization may also coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain. * Organizations may catalog lessons learned from every cyber incident. This lessons learned catalog should include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. * Organizations should conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. **Technical Requirements:**	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

			The organization implements a configurable capability to automatically disable critical information systems and/or accounts if security incidents are detected. * Organizations may implement 'Continuous' network, system, data, and storage information collection, and alert upon deviations from normal BASELINE asset behavior. **Barriers:** Lack of an Incident Response Plan will hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / and specialized technologies will hinder an effective response to an attack, breach or loss of data. False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to investigate the detection of cyber incidents.	
		RS.AN-3: Forensics are performed	**Operational Requirement(s):** The organization and appropriate staff may deploy a critical infrastructure information system which provides an audit reduction and report generation capability. Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. * Organizations may consider building a Security Team of staff with the following roles included, but not limited to: Incident Responders / Digital Forensics / Investigators / Security Leadership / Compliance Auditor / Legal Professional / Security Operations * Organizations can conduct frequent correlation of threat intelligence with collected network, system, data, and storage information. * Organizations may catalog lessons learned from every cyber incident. * This lessons learned catalog should include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:**	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4

			Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.. The report generation capability may be able to generate customizable reports. * Organizations may consider deploying big-data technologies to aid in the storage and processing of vast volumes of collected network/system data and information. * Organizations may conduct digital forensic activities to determine what / when / and how a detected cyber incident occurred. **Barriers:** Lack of an Incident Response Plan may hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / and specialized technologies will hinder an effective response to an attack, breach or loss of data. False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to investigate the detection of cyber incidents.	
		RS.AN-4: Incidents are categorized consistent with response plans	**Operational Requirement(s):** The organization and appropriate staff can track and document critical infrastructure information system security incidents. This may include maintaining records about the incidents, the status of the incidents, and how it was handling. * Organizations may catalog lessons learned from every cyber incident. This lessons learned catalog may include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. * Organizations may share and learn Threat, Attack, Signature, and remediation information with and from trusted organizations, government entities and trusted peers. **Technical Requirements:** Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers or other electronic databases of incidents.	· **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8

			Barriers: Lack of an Incident Response Plan will hinder an effective response to an attack, breach or loss of data. Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / specialized technologies will hinder an effective response to an attack, breach or loss of data.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	**Operational Requirement(s):** An organization and appropriate staff can coordinate incident handling activities with contingency planning activities. This may include coordinating with mission/business owners, information system owners, authorizing officials, human resources officials, and physical and personnel security offices. * Organizations can strive to identify a cyber incident as rapidly as possible and reach incident containment within 1 to 4 hours. Organizations may track and measure performance times and seek ways to reduce time to containment. **Technical Requirements:** Incident-related information may be obtained from a variety of sources, including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. * Organizations should be vigilant against Advance Persistent Threats (APTs) by implementing tools that constantly monitor for Attacker reconnaissance / Attacker incursion / Attacker response if discovered / Attacker capture of systems / Attacker outbound communications and stolen data transfer. **Barriers:** The hacker/attacker community has an endless capacity to advance their missions, methods and attack technologies. Organizations are left to often times guess a hacker's/attacker's next action and point of attack.	· **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents	**Operational Requirement(s):**	· **ISA 62443-2-**

		are mitigated	For critical infrastructure, appropriate and adequate Operations staff can implement incident handling measures for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The measures implemented may include lessons learned from ongoing incident handling activities. These measures should also be incorporated into training and testing exercises. * Organizations can strive to identify a cyber incident as rapidly as possible and achieve full business recovery and remediation within 1 to 24 hours. Organizations may track and measure performance times and seek ways to reduce time to Recovery. **Technical Requirements:** The organization adopts automatic mechanisms to support the incident handling process, for example, online incident management systems. The organization may also deploy dynamic reconfiguration of information systems to stop attacks, to misdirect attacks, and to isolate components of system. **Barriers:** Lack of an Incident Response Plan will hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / and specialized technologies will hinder an effective response to an attack, breach or loss of data. Numerous False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to investigate the detection of cyber incidents.	**1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**Operational Requirement(s):** For critical infrastructure, the organization and appropriate staff may develop a continuous monitoring strategy and implements a continuous monitoring program. The program may include a list of organization units to be monitored, the metrics in which to monitor them, and the frequency in which to employ such monitoring. * The organization and appropriate staff can update this risk assessments frequently or whenever there are significant changes to the information system. * Organizations can identify ~~all~~ possible threats and vulnerabilities to their assets, including, but not limited to: Unauthorized Access / Data Breaches / Malware / DDoS /	· **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5

			Advanced Persistent Threats / Zero-day Attacks / Phishing / SQL Injections / USB injected bots / and False alarms. * Organizations can catalog lessons learned from every cyber incident. This lessons learned catalog may include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:** The organization should employ vulnerability scanning tools and techniques. Organizations can employ these analysis approaches in a variety of tools, e.g. web-based applications scanners, static analysis tools, and binary analyzers. Vulnerability scanning includes, for example: (1) scanning for patch levels; (2) scanning for functions, ports, and protocols; (3) scanning for improperly configured or improperly operation information flow control mechanisms. **Barriers:** Lack of an Incident Response Plan will hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / and specialized technologies will hinder an effective response to an attack, breach or loss of data. Numerous False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to investigate the detection of cyber incidents.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous	**RS.IM-1:** Response plans incorporate lessons learned	**Operational Requirement(s):** The organization and appropriate staff should not only incorporate lessons learned from within the organization and particular organization groups, but should continually coordinate with external service providers to ensure that their capabilities are aligned with the organization. * Organizations can catalog lessons learned from every cyber incident. This lessons learned catalog can include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53**

	detection/response activities.		disabled / artifacts / compromised system accounts. **Technical Requirements:** Lessons learned may be documented and stored/placed in an area or directory where the organization's security staff can access. **Barriers:** Lack of an Incident Response Plan will hinder an effective response to an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / and specialized technologies will hinder an effective response to an attack, breach or loss of data. Numerous False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to investigate the detection of cyber incidents.	**Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	**Operational Requirement(s):** The organization and appropriate staff may revisit the developed response strategies on a scheduled basis and re-evaluate ongoing needs. This strategy may be constantly reviewed and approved by appropriate staff leaders. * Organizations may catalog lessons learned from every cyber incident. This lessons learned catalog may include, but not limited to: malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:** None **Barriers:**	. **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

			Numerous False alarms, lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to keep their response strategies up to date.	
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	**Operational Requirement(s):** The organization provides for the recover and reconstitution of the critical infrastructure information system to a known state after a disruption, compromise, or failure. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. * Organizations can strive to identify a cyber incident as rapidly as possible and achieve full business recovery and remediation within 1 to 24 hours. * Organizations may track and measure performance times and seek ways to reduce time to Recovery. **Technology Requirement(s):** The organization may consider DR technologies, systems, protocols, networks, off-site data storage facilities, and services. There may be more than adequate storage capacity, database capacity, and network bandwidth to allow frequent backups of critical information and data. * Organizations may wish to consider implementing complete full-scale disaster recovery technologies and service providers. **Barriers:** There will be an additional CAPEX cost to procuring DR technologies and off-site services like storage and data recovery. There will be an additional OPEX cost to allocate, hire, train staff to be responsible for Business Continuity and Disaster Recovery	· **CCS CSC** 8 · **COBIT 5** DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future	**RC.IM-1:** Recovery plans incorporate lessons learned	**Operational Requirement(s):** The organization and appropriate staff should not only incorporate lessons learned from within the organization and particular organization groups, but should continually coordinate with external service providers to ensure that their capabilities are aligned with the organization. * Organizations can catalog lessons learned from every cyber incident and how the business functions were recovered. This lessons learned catalog can include, but not limited to: Business Continuity(BC) / Disaster Recovery (DR) / malware	· **COBIT 5** BAI05.07 · **ISA 62443-2-1** 4.4.3.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

	activities.		behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:** BC/DR Lessons learned may be documented and stored/placed in an area or directory where the organization's security staff can access. **Barriers:** Lack of BC/DR Plans will hinder an effective recovery from an attack, breach or loss of data. * Lack of internal cyber security expertise in the areas of investigation / security analysis / forensics / incident response / and BC-DR technologies will hinder an effective recovery from an attack, breach or loss of data. Lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to recover from cyber incidents.	
		RC.IM-2: Recovery strategies are updated	**Operational Requirement(s):** For critical infrastructure, appropriate and adequate Operations staff may implement incident handling measures for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The measures implemented should include lessons learned from ongoing incident handling activities. These measures may also be incorporated into training and testing exercises. * Organizations may catalog lessons learned from every cyber incident and how the business functions were recovered. This lessons learned catalog may include, but not limited to: Business Continuity(BC) / Disaster Recovery (DR) / malware behaviors / attacker activities during compromise / network-system-data anomalies and deviations from the BASELINE / Applications and software that can be disabled / artifacts / compromised system accounts. **Technical Requirements:**	· **COBIT 5** BAI07.08 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

			Automated technology can be implemented to support the incident handling process. For example, online incident management systems. The organization may also employ dynamic reconfiguration tools that are able to reconfigure information systems if and when an attack occurs. **Barriers:** Lack of dedicated security staff, lack of staff availability, and lack of budget all could affect the organizations ability to keep their Business Continuity and Disaster Recovery strategies up to date.	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	**Operational Requirement(s):** For critical infrastructure, the organization and supporting staff can identify external compliance requirements and review, and adjust policies, principles, standards, procedures and methodologies to ensure that legal regulatory, privacy and contractual requirements are addressed and communicated. * Organization may determine the consequences of various cyber incidents. These consequences may include, but not limited to degradation of public trust / financial and market losses / degradation of brand reputation / impact to critical infrastructure. * Organizations may have appropriate press releases and official notifications prepared and delivered in a timely manner following a cyber incident. * Organizations can follow Industry standards, codes of good practice, and best practice guidance for adoption and adaptation. **Technical Requirements:** None **Barriers:** Some staff, executives, shareholders and board members may disagree with the content and delivery time of press releases and official notifications.	· **COBIT 5** EDM03.02
		RC.CO-2: Reputation	**Operational Requirement(s):**	· **COBIT 5**

		after an event is repaired	For critical infrastructure, the organization and supporting staff may identify external compliance requirements and review, and adjust policies, principles, standards, procedures and methodologies to ensure that legal regulatory and contractual requirements are addressed and communicated. * Organization can determine the consequences of various cyber incidents. These consequences may include, but not limited to degradation of public trust / financial and market losses / degradation of brand reputation / impact to critical infrastructure. * Organizations can have appropriate press releases and official notifications prepared and delivered in a timely manner following a cyber incident. * Organizations can follow Industry standards, codes of good practice, and best practice guidance for adoption and adaptation. **Technical Requirements:** None **Barriers:** Some staff, executives, shareholders and board members may disagree with the content and delivery time of press releases and official notifications.	MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**Operational Requirement(s):** The appropriate staff and organization leaders may identify essential missions and business functions and their associated contingency requirements. The organization then can provide contingency roles and responsibilities to the appropriate individuals. Once finalized, the organization may distribute copies of this plan, update the plan as need be, and protect the plan from unauthorized disclosure or modification. * The organization can determine "who-internally" needs to know "what" information, "when" and "how" will that information be delivered. The organization can take into account "all" internal communications with: Tiers I,II,III of operations, network ops centers, engineering, technical management, program/project management, customer service, IT, sales, C-suite officials, billing, accounting, human resources, security offices etc. * Once these communication paths and flows have been determined the organization may set access controls- business process rules within various	· **NIST SP 800-53 Rev. 4** CP-2, IR-4

			systems to allow authorized personnel to reach their required information, when they need it to perform their job function. * The entire flow of information that describes who-what-when-how should be documented and conveyed through ongoing training, to the effected personnel. **Technical Requirements:** The organizations can ensure that secure, reliable electronic communications (email, text, voice comms....., etc.) are in place, so that appropriate personnel are alerted into action when an incident response is required. **Barriers:** There may be an additional OPEX and CAPEX costs associated with back-up/redundant services from service providers and trusted 3rd parties who may be needed in response to an incident. Lack of formal, and Ad-Hoc communications between sub-organizations, suppliers, and service providers before, during and in response to a cyber incident, will hinder any effective incident response.	

9.7 CYBER ECOSYSTEM AND DEPENDENCIES
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY

Communications in today's world, takes on numerous meanings, over numerous types of networks, through numerous technologies. To explain today's communications ecosystem, one has to use diagrams, graphics and text in order to capture and explain all of the nuances in today's complicated communications environment. The CSRIC IV-WG4 ecosystem work products were developed and drafted based on the types of experiences that consumers, businesses, and governments experience through their use of the Internet and the public switched telephone networks. The textual and graphical ecosystem representations included in this document are devoid of any competitive, regulatory, political or economic characteristics of today's communications environment.

It is recommended that a deeper investigation, a larger data gathering and graphing effort take place to compare the weight of the economic and socio-economic impacts that each ecosystem category and major players have on society, in order to fully describe our communications ecosystem.

II. INTRODUCTION

The Ecosystem Feeder group of the CSRIC IV – Working Group 4, was tasked with graphically and textually depicting the Internet Ecosystem, so that the greater CSRIC IV- WG4 can use this work product as tools in their individual segment analysis. This overall ecosystem depiction is to also include Communications Sector specific dependencies on other ecosystem categories and factors that will aid in keeping the Communications Sector cyber-secure.

III. FEEDER GROUP STRUCTURE

The Ecosystem Feeder Group consists of the members listed below.

Name	Company
Co-Chair: Thomas Soroka Jr	USTelecom
Co-Chair: Brian Scarpelli	TIA
Vern Mosley	FCC
Mike Alagna	Motorola
Nadya Bartol	Utilities Telecom Council
Jim Bean	Juniper Networks
Chris Boyer	AT&T
Joel Capps	Ericsson
Inette Furey	DHS
Stacy Hartman	CenturyLink
Joe Viens	Time Warner Cable
Danna Valsecchi	Verizon
Rao Vasireddy	Alcatel-Lucent
Matt Tooley	NCTA
Christian Vogler	Gallaudet University
Ray Singh	ACS
Kate Dean	USISPA

Table 2 - List of Working Group Members

IV. BACKGROUND

The foundational objective of the CSRIC IV- WG4 is to address the question:

How will CSRIC IV-WG4's product help companies in the five Communications Sector segments contribute to their capacity to assure appropriate internal and external stakeholders of the sufficiency of their own cyber risk management practices?

V. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objectives

Drawn from the above stated WG4 objective, the ecosystem feeder group's primary objective is to depict the Internet and Communications ecosystem via graphic and textual "tools", such that the WG4 segments and subgroups can easily identify where their segments fit into the Ecosystem and can ensure that their analysis considers all aspects of the Internet and Communications ecosystem.

A secondary objective of the ecosystem feeder group is to analyze what cyber-security dependencies exist between the Communications Sector and other aspects of the Internet and communications Ecosystem. The work product deliverables of the ecosystem feeder group are to be used as tools by the WG4 segments and subgroups in their analysis.

B. Scope

The ecosystem feeder group is tasked with delivering graphical and textual depictions of the Internet ecosystem, Communications Sector cybersecurity dependencies, and a mapping of network layers to ecosystem categories and to cyber-attacks and threats.

Ecosystem Graphic Depictions: The Ecosystem team looked at several ways to graph, diagram and graphically depict the Internet and Communications ecosystem. The Ecosystem team also looked at previous work done by various entities within private industry and the U.S. Government to depict the Internet and Communications ecosystem. You will find all of the chosen Ecosystem graphic depictions in **Appendix-A** of Section VIII of this document.

Ecosystem Category Descriptions: Once the Ecosystem categories were identified, the ecosystem feeder group drafted descriptions for every identified category. These descriptions focused on what functions the companies in these categories conducted, how they delivered their services and several examples of real world providers in each category. You will find all of the Ecosystem category descriptions in **Appendix-B** of Section VIII of this document.

Ecosystem & Communications Sector Dependencies: Following the Ecosystem Category identification exercise, the Ecosystem team looked at each individual category and listed what that particular category depended on to make it cyber secure. We answered the question *"If I were an Ecosystem Category, What would I depend on to*

keep me cyber secure?" After we determined the dependencies for each of the Ecosystem categories, we narrowed the dependencies down to only the Communications Sector. The ecosystem feeder group answered the question:

"*If I were a member of the Communications Sector, what other Ecosystem categories would I depend on to keep me Cyber secure?*"

You will find the Communications Sector dependencies in the Results and Findings Section VI of this document.

Ecosystem Category Mapping to TCP/IP Layers and Cyber Attacks: Following the dependency exercise, the ecosystem feeder group conducted the following:

- Identified the major network and computing protocols that resided in each of the TCP/IP model layers.
- Mapped all of the identified Ecosystem categories to one or more TCP/IP layers, depending on where these categories operated in the Ecosystem. Some categories operate in a single TCP/IP layer, while some categories operate in multiple layers of the TCP/IP model.
- Mapped known cyber-attacks, threats and breaches to specific layers of the TCP/IP model, based on what protocols or layers were attacked and exploited.
- Created a '*Definitions Key*', for the reader to understand the various acronyms used in this chart.

This mapping chart can be read in several ways. When starting with cyber-attacks and threats, they are associated with specific networking and computing protocols, so a particular *Attack* or *Threat* and its *Vector* can be seen on this chart. Any service provider that operates in one or more of the TCP/IP layers or those set of protocols, should be aware of these types of attacks. The CSRIC W4 will determine potential actions and possible best practices for these service providers to consider.

Another way of reading this chart starts with the Ecosystem categories listed in the left column. The Ecosystem categories listed are associated with various specific networking and computing protocols, so a particular Ecosystem category can identify which known cyber-attacks have taken place in its operating space. Any service provider that operates in one or more Ecosystem categories should be aware of these types of attacks. The CSRIC W4 will determine potential actions and possible best practices for these service providers to consider.

You will find the Ecosystem-TCP/IP layers-Cyber Attack mapping in the Results and Findings in Section VI of this document.

C. Methodology

The ecosystem feeder group began this effort by identifying as many Internet and communications companies as possible, (labeled as 'Players') that affected the lives of

consumers, businesses, and governments. If a large number of players were identified to operate in a single category, then they were consolidated into that given category. These 'players' were listed in column A of a spreadsheet.

The ecosystem feeder group then proceeded to identify major Ecosystem categories like; access providers, backbone network operators, hardware vendors, operating system vendors etc. These Internet and communications ecosystem categories were listed across row A in the same spreadsheet as the previously identified players.

The ecosystem feeder group proceeded to check for intersecting cells in this spreadsheet to determine what categories the major 'players' operated in, and applied a color to the intersecting cells in this spreadsheet. It soon became very graphically obvious that, many large well-known companies operate in many categories across our communications ecosystem. Some even operated from operating systems all the way through fiber backbone network operators.

Once the Internet and Communications ecosystem categories were identified and vetted by the group, the next task was to identify the individual category dependencies, by answering the question: *"If I were an Ecosystem Category, What would I depend on to keep me cyber secure?"*

The ecosystem feeder group then proceeded to focus on the Communications Sector ecosystem categories and identified their specific cybersecurity dependencies on the remaining ecosystem categories. The Communications Sector categories were listed across Row A of a new spreadsheet and the remaining ecosystem categories were listed in column A of this new spreadsheet. The ecosystem feeder group identified Communications Sector dependencies by answering the question: "*If I were a member of the Communications Sector, what other Ecosystem categories would I depend on to keep me Cyber secure?*"

It soon became very graphically obvious that, the Communications Sector relied on numerous other ecosystem categories to keep itself, as a sector, cyber secure.

VI. RESULTS AND FINDINGS

The Internet and communications ecosystem is a constantly growing, rapidly changing, complex system of suppliers, networks and consumers that requires continuous attention to the security of its components and availability to its end users.

The ecosystem feeder group identified 27 unique Ecosystem categories like; access providers, backbone network operators, hardware vendors, operating system vendors etc. It became very graphically obvious that, many well-known companies operate in numerous categories across the Internet and Communications ecosystem. Some even operated in diverse areas that ranged from operating systems all the way through fiber network operations. These companies serve a multitude of critical functions across the Internet and communications experiences of consumers, enterprises, and government entities alike.

Cyber-attacks have been observed and mapped to every layer of the TCP/IP communication model, and subsequently against every identified category of the ecosystem.

Cyber-attacks will continue to occur at every level of the TCP/IP communications model. It is imperative that all operators and vendors in every layer of the TCP/IP model conduct their operations with the highest level of cyber security diligence, to prevent crippling attacks on their own operations and/or passing potential threats through their communications layer and possibly crippling adjacent entities within the ecosystem.

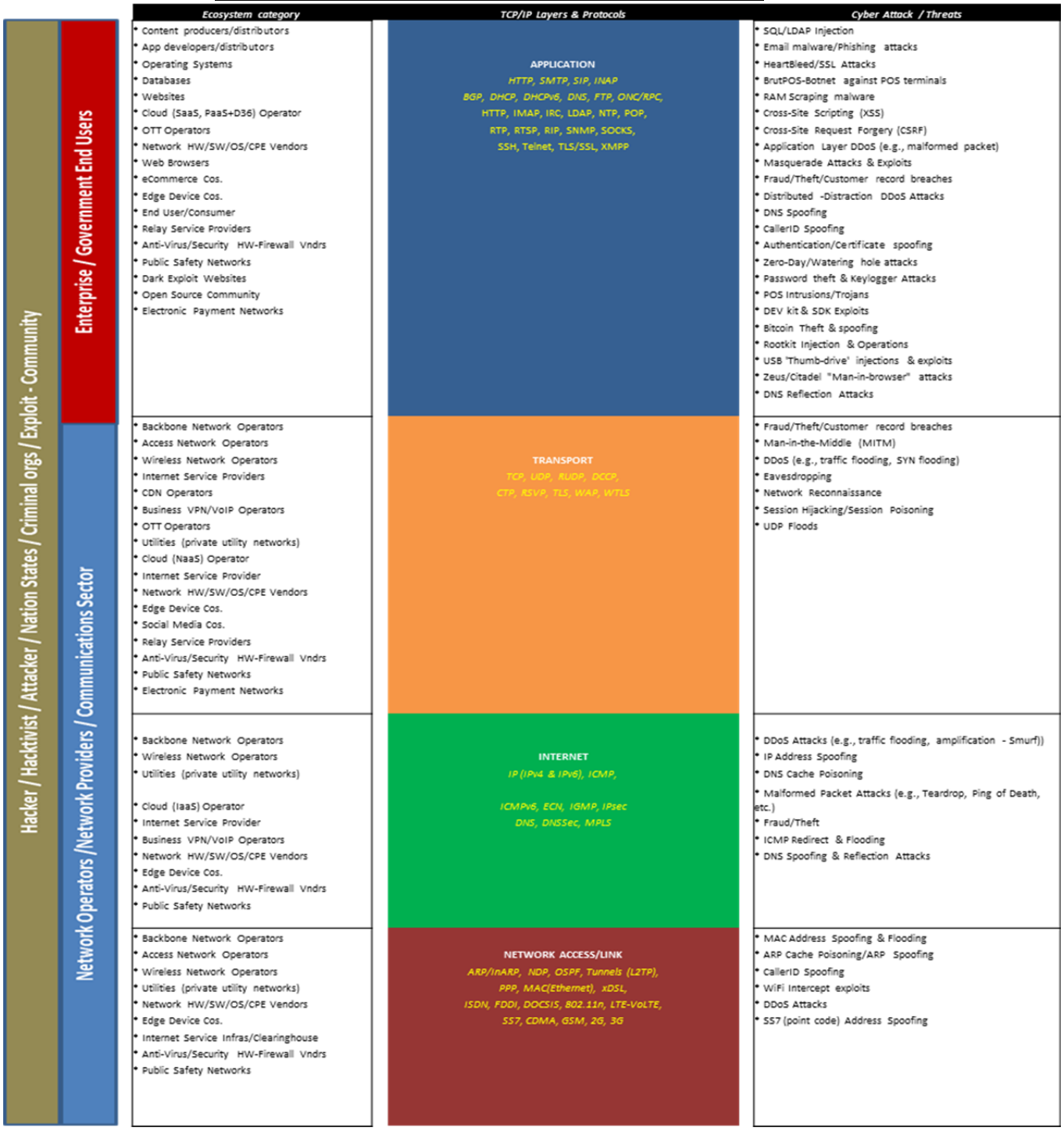
The Communications Sector depends on multiple non-Communications Sector ecosystem categories to make itself and its end users cyber secure.

As a result of the research and analysis conducted by the ecosystem feeder group conducted within the timeline of the CSRIC IV-WG4, the following observations, results and findings were made.

- Several companies occupy numerous ecosystem categories ranging from operating system vendors, device vendors through fiber access network operators. Since these companies serve a multitude of critical functions across the Internet and communications experiences of consumers, enterprises, and government entities, they must conduct all of their operations in a cyber-secure manner, or risk attacks that could cripple their operations, and negatively impact their line of business.

- Cyber-attacks have occurred and will continue to occur at every level of the TCP/IP communications model. It is imperative that all operators and vendors in every layer of the TCP/IP model conduct their business and operations with the highest level of cyber security diligence, or risk having attacks cripple their own operations and/or pass through their communications layer and possibly cripple adjacent entities within the ecosystem. Cyber-attacks have been observed at every layer of the TCP/IP communication model, and subsequently against every category of the ecosystem, as seen in this chart and definitions below:

Ecosystem to TCP/IP Layers to Cyber Attack Mapping



Definitions Key:

Acronym/Term	Descriptions	Source
DDoS	Distributed denial-of-service (DDoS) attacks are sent by two or more persons, or bots	http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_a
SQL	Originally based upon relational algebra and tuple relational calculus, SQL consists of adata definition language and a data manipulation language. The scope of SQL includes data insert, query, update and delete, schema creation and modification, and data access control.	http://en.wikipedia.org/wiki/SQL
LDAP	The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.	http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protoco
Zero-Day Attack	A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, one that developers have not had time to address and patch.[1] It is called a "zero-day" because the programmer has had zero days to fix the flaw.	http://en.wikipedia.org/wiki/Zero-day_attack
DEV	Dev or indev software, applications or other pieces of computer software still in alpha or beta stages of development, or alternatively, a neutral build or nightly build, a version of a software which represents the current state of its source code, which could be unstable or buggy	http://en.wikipedia.org/wiki/Dev#Technology
SDK	A software development kit (SDK or "devkit") is typically a set of software development tools that allows the creation of applicationsfor a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform.	http://en.wikipedia.org/wiki/Software_development_kit
Rootkit	A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.	http://en.wikipedia.org/wiki/Rootkit
Man-In-Middle Attack	The man-in-the-middle attack (often abbreviated MITM, MitM, MIM, MiM, MITMA) in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.	http://en.wikipedia.org/wiki/Man-in-the-middle_attack
DNS	The Domain Name System (DNS) translates easily memorized domain names to the numericalIP addresses needed for the purpose of locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet.	http://en.wikipedia.org/wiki/Domain_Name_System
ICMP	The Internet Control Message Protocol (ICMP) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.	http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
MAC Address Spoofing	MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing.	http://en.wikipedia.org/wiki/MAC_spoofing
ARP Spoofing	ARP spoofing is a technique whereby an attacker sends fake ("spoofed")Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP addressof another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.	http://en.wikipedia.org/wiki/ARP_spoofing
UDP	With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths.	http://en.wikipedia.org/wiki/User_Datagram_Protocol
POS	Point of sale (also called POS or checkout) It is the point at which a customer makes a payment to the merchant in exchange for goods or services.	http://en.wikipedia.org/wiki/Point_of_sale
SYN Flood	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.	http://en.wikipedia.org/wiki/SYN_flood
SSL	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over the Internet.	http://en.wikipedia.org/wiki/Secure_Sockets_Layer
SS7	Signalling System No. 7 (SS7) is a set of telephony signaling protocols which are being used to set up most of the world's public switched telephone network (PSTN) telephone calls. The main purpose is to set up and tear down telephone calls. Other uses include number translation, local number portability, prepaid billing mechanisms, short message service (SMS), and a variety of other mass market services.	http://en.wikipedia.org/wiki/Signalling_System_No._7
DNS Reflection/Redirection	DNS hijacking or DNS redirection is the practice of subverting the resolution of Domain Name System (DNS) queries. This can be achieved by malware that overrides a computer's TCP/IP configuration to point at a rogue DNS server under the control of an attacker, or through modifying the behaviour of a trusted DNS server so that it does not comply with internet standards.	http://en.wikipedia.org/wiki/DNS_hijacking

The Communications Sector depends on multiple non-Communications Sector ecosystem categories to make itself and end users cyber secure, as seen in this chart below:

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

VII. CONCLUSIONS AND RECOMMENDATIONS

The charter of the CSRIC IV-WG4 ecosystem feeder group was to depict the Internet and communications ecosystem and determine Communications Sector cyber-security dependencies. The conclusions that can be drawn from the work that was completed by this feeder group are as follows:

- The Internet and communications ecosystem is a constantly growing, rapidly changing, complex system of suppliers, networks and consumers that requires continuous attention to the security of its components and availability to its end users.

- The ecosystem feeder group identified 27 unique Ecosystem categories like; access providers, backbone network operators, hardware vendors, operating system vendors etc. It became very graphically obvious that, many well-known companies operate in numerous categories across the Internet and Communications ecosystem. Some even operated in diverse areas that ranged from operating systems all the way through fiber network operations. These companies serve a multitude of critical functions across the Internet and communications experiences of consumers, enterprises, and government entities alike.

- Cyber-attacks have been observed and mapped to every layer of the TCP/IP communication model, and subsequently against every identified category of the ecosystem.

- Cyber-attacks will continue to occur at every level of the TCP/IP communications model. It is imperative that all operators and vendors in every layer of the TCP/IP model conduct their operations with the highest level of cyber security diligence, to prevent crippling attacks on their own operations and/or passing potential threats through their communications layer and possibly crippling adjacent entities within the ecosystem.

- The Communications Sector depends on multiple non-Communications Sector ecosystem categories to make itself and its end users cyber secure.

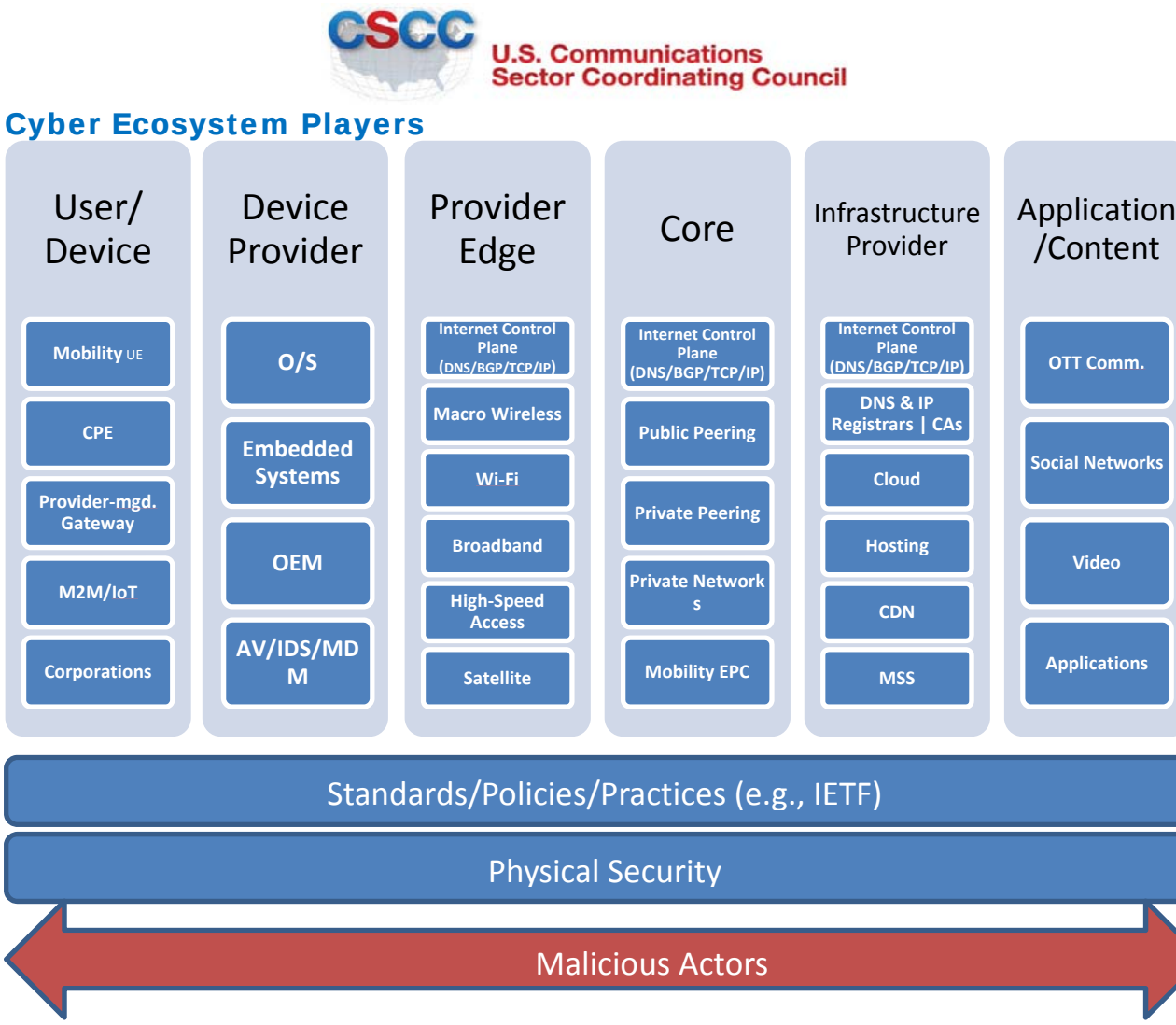
- It is recommended that further Internet and communications ecosystem studies be conducted to include the number of end users of each ecosystem player and category, and to determine social, governmental and economic impacts of the Internet and Communications ecosystem and its availability.

VIII. APPENDICES

A. APPENDIX – A Graphical Depictions of the Internet and Communications Ecosystem

One of the more comprehensive 'Ecosystem' diagrams comes from a joint industry/government partnership called the U.S. Communications Sector Coordinating Council (CSCC). The ecosystem feeder group determined that this diagram captured a large number of the categories of the Ecosystem that were previously identified and it was an excellent depiction of the various 'Cyber' Ecosystem relationships within the Communications Sector. This CSCC diagram was shared with the ecosystem feeder group and is shown below:

Communications Sector Coordinating Council:
Cyber Ecosystem Players

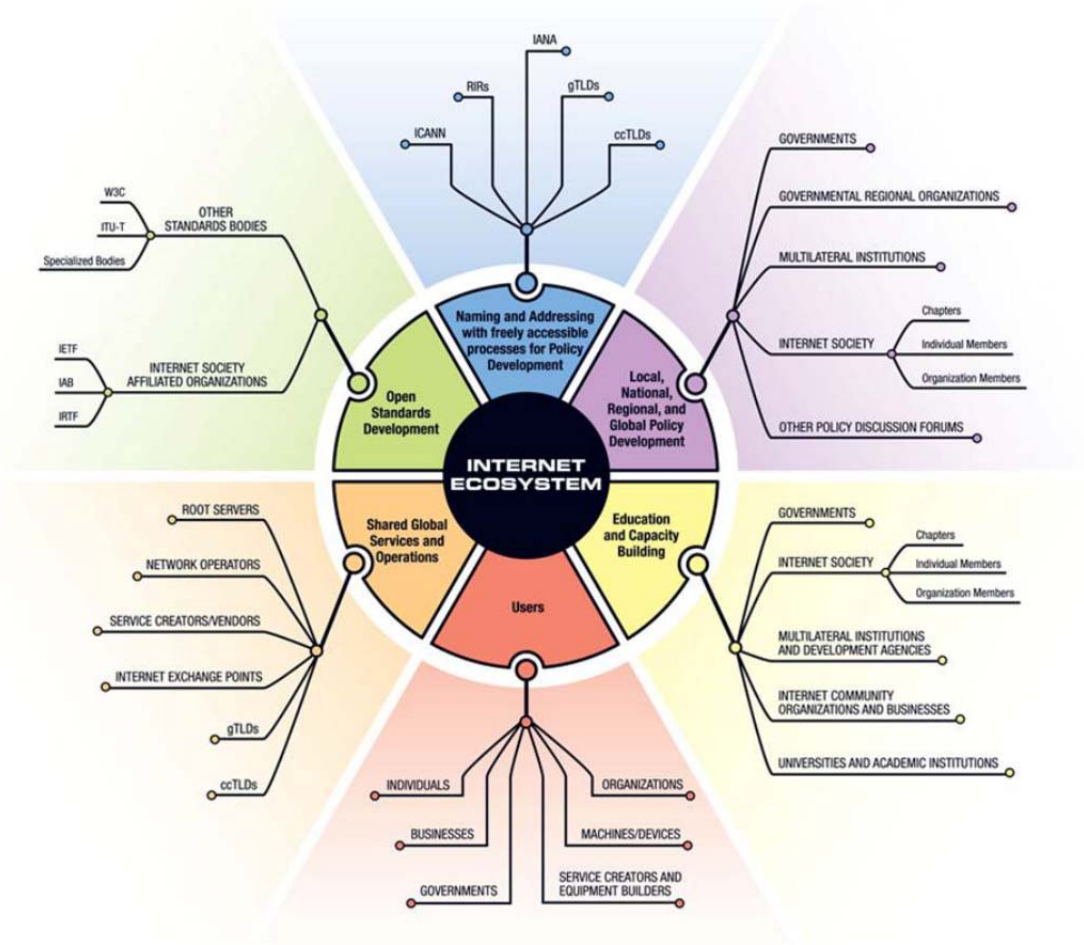


The ecosystem feeder group analyzed numerous 'ecosystem' diagrams developed by several industry-governments working groups and selected several comprehensive

diagrams. These graphic depictions of the Internet & Communications Ecosystem are to be used as tools to understand various categories, players and the roles they play in our Internet experiences. The sources of these Ecosystem diagrams are listed above each diagram, and the unique information that can be drawn from each diagram is below each diagram.

The Internet Ecosystem: Internet Society

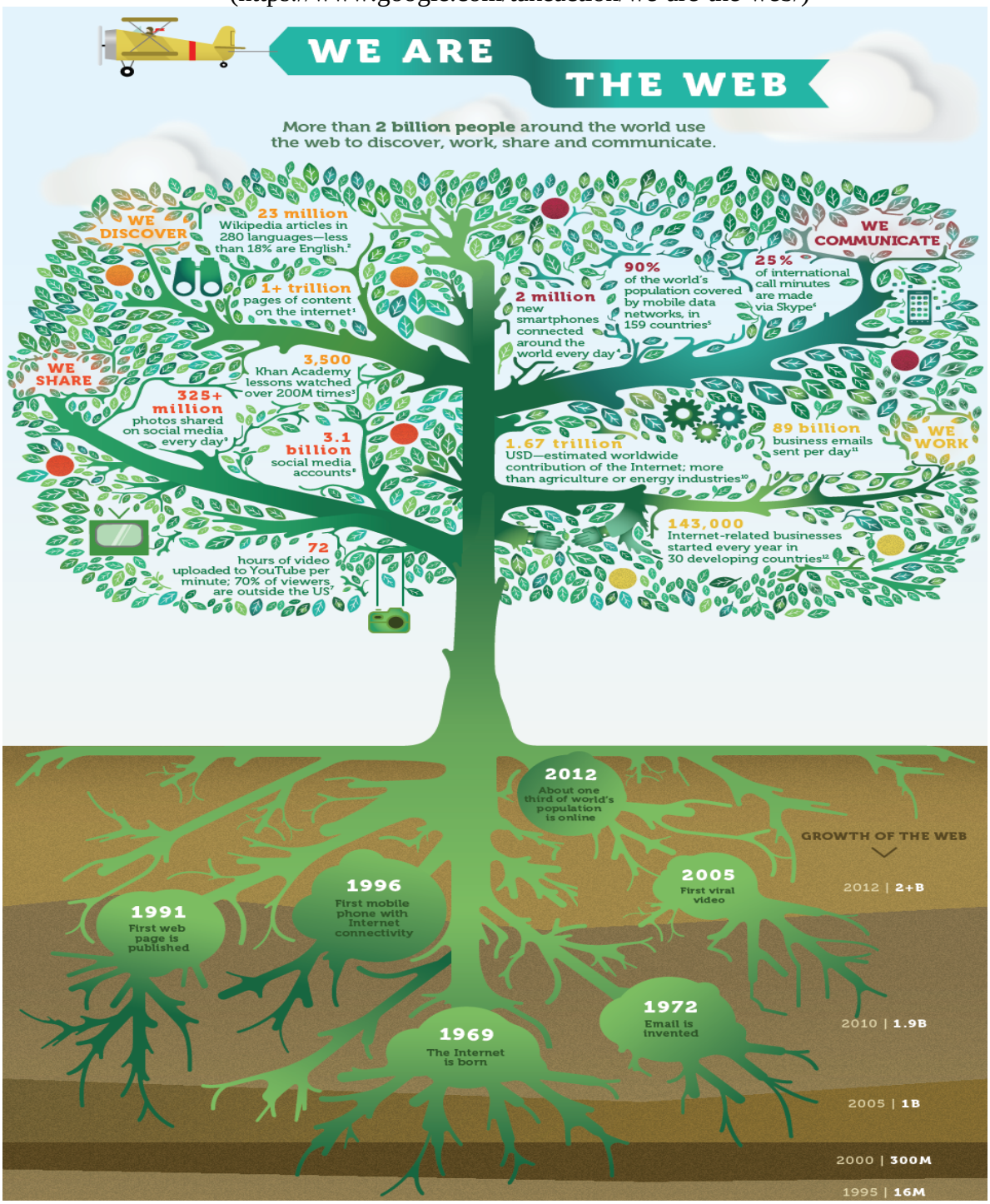
(http://www.isoc.org)



This ISOC diagram of the Internet Ecosystem shows the various 'influences' and 'influencers' of the Internet. The Internet Engineering Task Force (IETF), made up of international participants, has developed the critical protocols, and approved standards that enable the Internet to operate and communicate on a truly global scale.

We Are the Web: Google

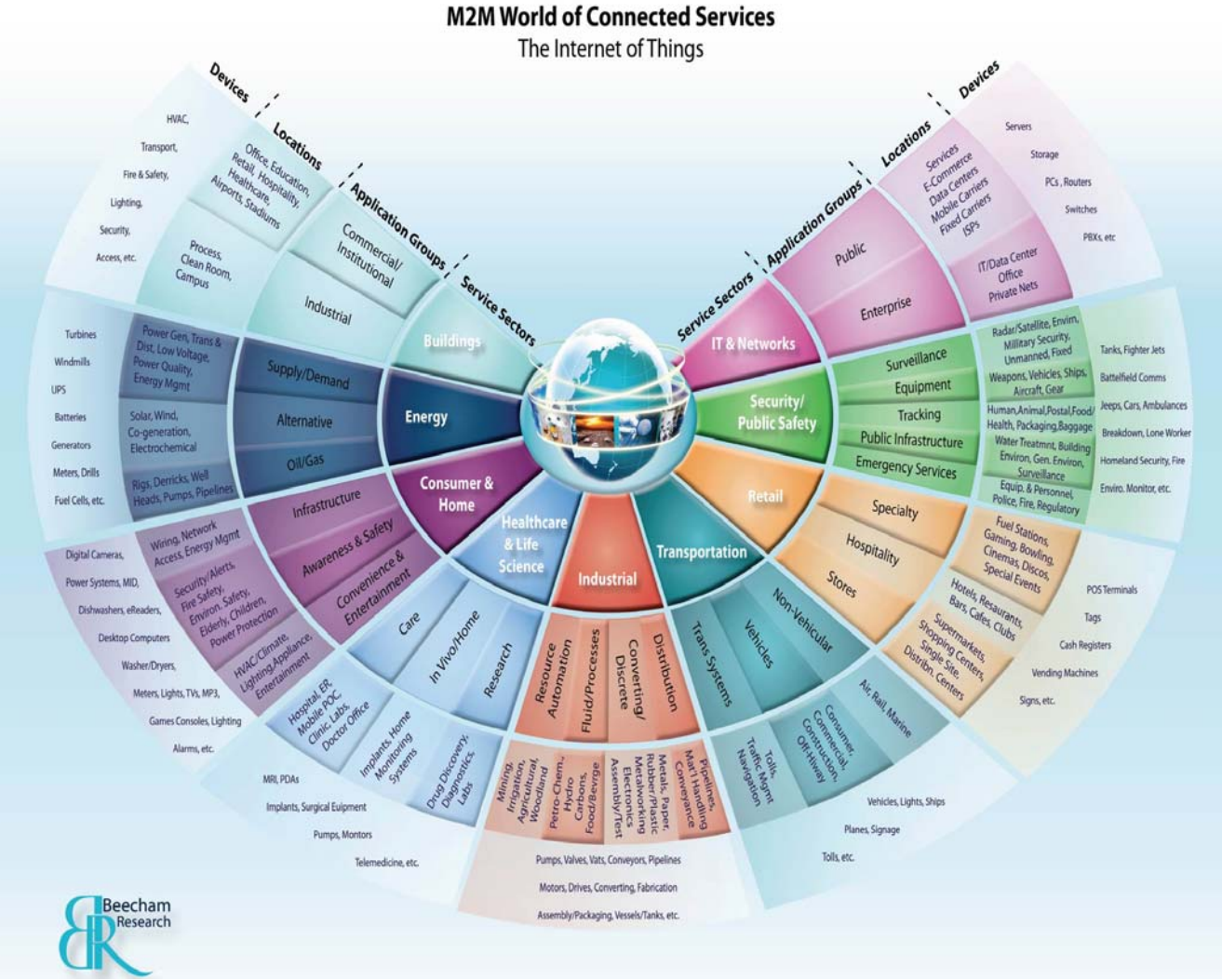
(https://www.google.com/takeaction/we-are-the-web/)



This diagram from Google depicts the Internet's ever growing roots and timeline of growth along with the massive scales of the various users, producers, and communicators of the global Internet tree.

Beecham Research: Internet of Things

(http://beechamtech.com/wp-content/uploads/2013/10/M2M1.jpg)



This diagram from Beecham Research breaks the Internet Ecosystem into Service Sectors, Application User-groups, Locations and End-user physical devices. This diagram is a great depiction of the ever growing "Internet of Things" (IoT). The more of these devices and technologies we develop, the more they become connected to the global Internet.

Federal Communications Commission: National Broadband Plan-
(http://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf)

Exhibit 3-A:
Forces Shaping the Broadband Ecosystem in the United States

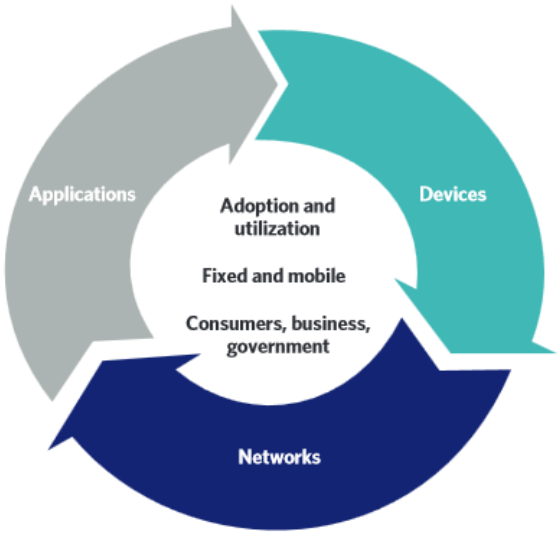
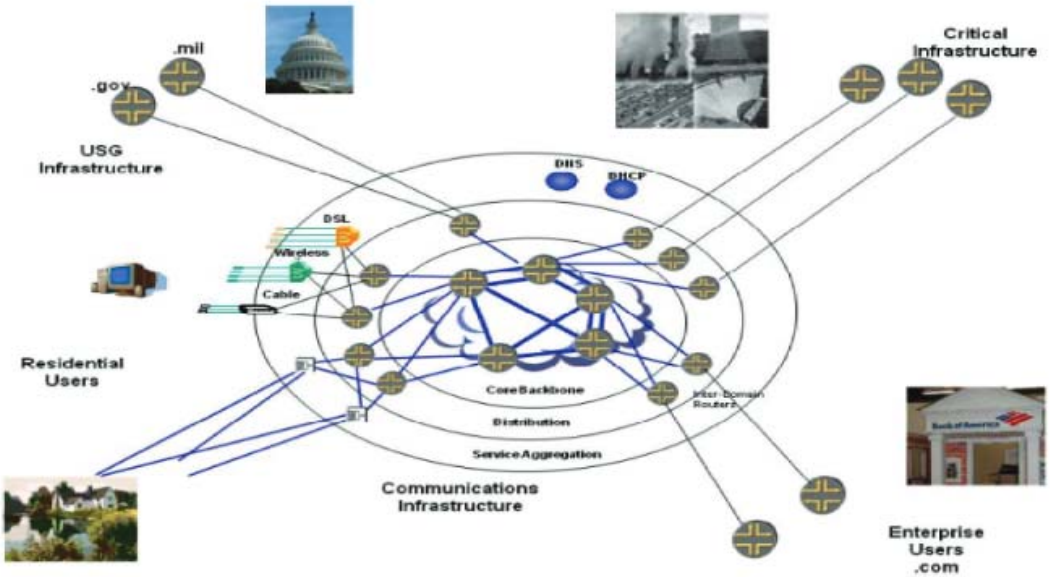


Exhibit 16-D:
The Cyber World

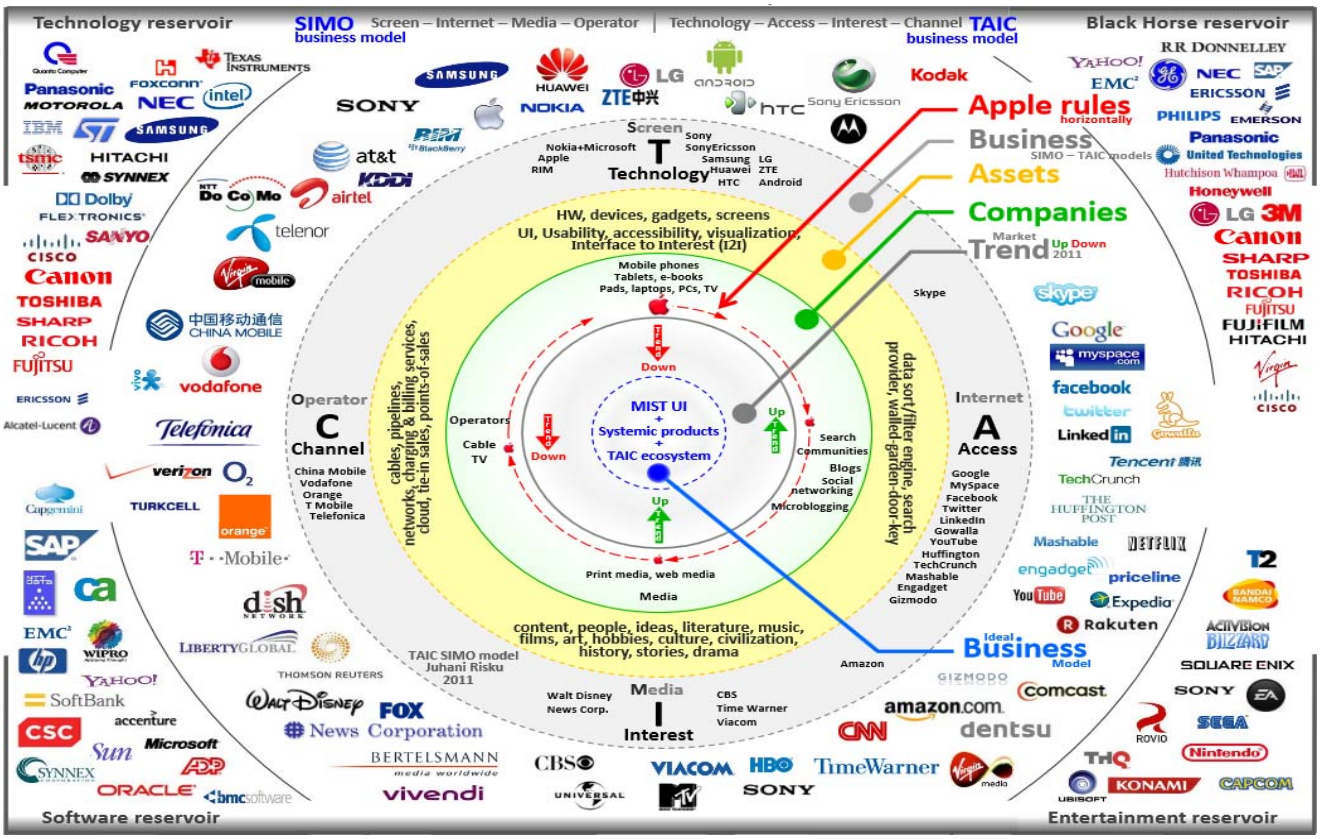


These two diagrams depict the Internet and Broadband Ecosystem from the perspective of the F.C.C. and the National Broadband Plan. It shows the relationship between the publicly available Internet and the critical infrastructure that is needed to serve the population with critical government functions. The concentric circles also show the various layers upon which communications and services begin their journey with access to networks, they get aggregated onto larger networks, and ultimately transported over critical, high capacity backbone networks.

Technology, Access, Interest, Channel / Screen, Internet, Media, Operator Model:

Juhani Risku

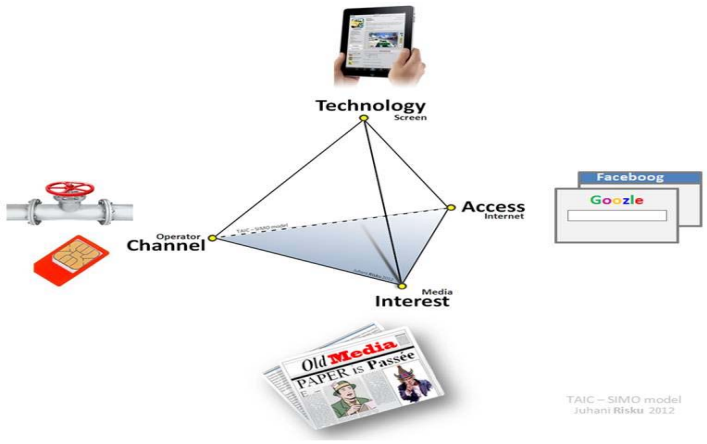
(http://abstractionshift.files.wordpress.com/2011/10/11_taic_simo_technology-access-interest-channel_screen-internet-media-operator_businesses_logos_juhani_risku_2011.pdf)



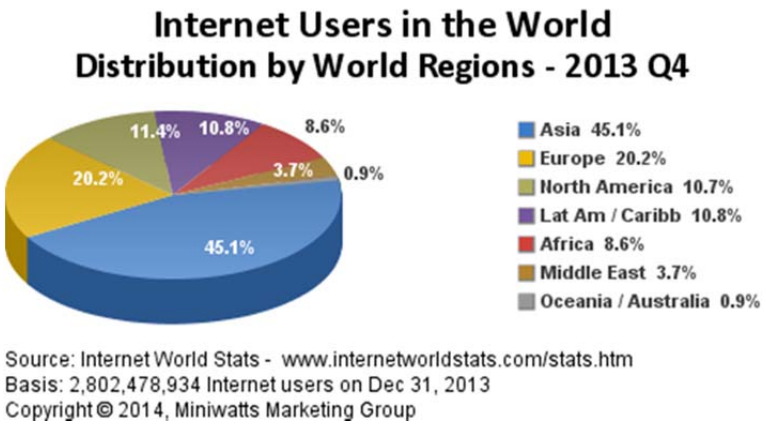
This diagram developed by Juhani Risku also shows the various layers that make up the Internet Ecosystem, but the actual companies and corporations that touch our Internet lives are also shown in this diagram. It's very important to observe that various companies land in multiple layers of the Ecosystem and cannot be characterized as a single "type" of company.

TAIC-SIMO Operator/Network Model:

Juhani Risku-
(http://interestmachine.wordpress.com/taic-simo-model/operator-network-model/)



Another diagram from Juhani Risku, simplifies the more complex ecosystem diagrams into a much smaller subset of building blocks that make up the Internet Ecosystem. Our interests dictate what type of media (TV, Radio, Email, Internet, Text, Social Media etc.) we wish to use to consume these interests. The media that we choose dictates what types of technologies and networks we wish to buy and use. The technologies that we choose to use, will dictate the types of access required, and through what channels this access can be obtained.



This pie chart shows the global consumption of the Internet Ecosystem, and the demand for Internet access across the globe.

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.

2) Access Network Operators

Cable Operators, also known as multi-system operators (MSOs) are service providers that in whole or in part receive signals transmitted or programs broadcast by one or more television broadcast stations licensed by the FCC, and makes secondary transmissions of such signals or other programs by wires, cables, microwave, or other communications channels, as well as other content received via satellite, to subscribing members of the public who pay for such service. Examples of Cable Operators include Comcast, Time-Warner Cable, and Cox Communications.

xDSL refers to the sum total of digital subscriber line (DSL) technologies that utilize telephone exchanges to provide Internet transmissions to subscribers of the service. xDSL typically provides “last-mile technologies”; i.e. are used between a telephone switching station and a home or office, and not between switching stations; and vary in transmission methods based on the service provider, equipment used, geographical location and the customer.

Fiber To The Node (FTTn) is defined as optical fiber to a node in an area to provide a group of subscribers with Internet service, with the “last-mile” connection typically provided via xDSL or coaxial copper wire. FTTn solutions use a hybrid configuration to deliver data over more efficient fiber optic lines for the majority of the data transmission while utilizing already existing connections to subscribers from local nodes. Examples of FTTn operators include AT&T’s U-verse and Verizon FiOS.

WiFi is a wireless local area network (WLAN) that is based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standard series. Wi-Fi allows an electronic device to exchange data or connect to the Internet using 2.4 GHz UHF

and 5 GHz SHF radio waves, and in this way typically provide wireless "last-mile" connectivity. Examples of Wi-Fi applications include free Wi-Fi connectivity at businesses such as Starbucks and Panera Bread.

Satellite Operators are service providers that enable service to subscribers for a fee utilizing satellite transmissions from base stations to end users. In this way satellite operators provide television, voice, and Internet service to end-users. Examples of satellite operators include Globalstar and Intelsat.

3) Wireless Network Operators

Wireless Network Operators are entities which operate wireless networks, be they licensed or unlicensed. Wireless networks provide connectivity over

Mobile Network Operators are wireless communications service providers that own or control the necessary network components to sell and deliver services to an end user. These components include radio spectrum allocation, wireless network infrastructure, backhaul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organizations. Examples of MNOs are AT&T, Sprint, T-Mobile and Verizon Wireless.

Mobile Virtual Network Operator (MVNO) are companies that provides mobile phone services, but do not have their own licensed frequency allocation of radio spectrum, nor the infrastructure required to provide mobile telephone service. A MVNO attains access through agreements with mobile network operators to obtain bulk access to network services at wholesale rates, and then sets retail prices independently. Examples of MVNOs are 420 Wireless, Boost Mobile, and Cricket Wireless.

4) Internet Service Providers

Internet Service Providers (ISPs) are the businesses and organizations that provide users with Internet access and related services. ISPs typically provide telecommunications services including data communications access and telephone connection. Examples of ISPs include Comcast, AT&T, and Comcast. There are numerous types of ISPs:

- **i.** Access ISPs employ a variety of technologies to facilitate consumers' connection to their network. These technologies may include broadband or dialup. Always-on types of broadband connections comprise cable, fiber optic service (FiOS), DSL (Digital Subscriber Line) and satellite. A number of access providers also provide email and hosting services.
- **ii.** Mailbox ISPs offer email mailbox hosting services and email servers to send, receive and store email. Many mailbox ISPs are also access providers.
- **iii.** Hosting ISPs offer email, File Transfer Protocol (FTP), web-hosting services, virtual machines, clouds and physical servers.
- **iv.** Transit ISPs provide large amounts of bandwidth needed to connect hosting ISPs and access ISPs together.

v. Virtual ISPs (VISP) purchase services from other ISPs to allow customers Internet access.

vi. Free ISPs (freenets) provide service free of charge and often display advertisements while users are connected.

5) Content Delivery Network (CDN) Operators

Content Delivery Network (CDN) operators are companies that provide services to improve network performance by distributing content to cache or edge servers located geographically close to users, which deliver copies of content to end-users.[71] CDN operator services maximize bandwidth, improve accessibility and maintain correctness through content replication, offering fast and reliable applications and services through some combination of content-delivery, request-routing, distribution and accounting infrastructure. Examples of CDN operators include Akamai, Limelight, Level3, Verizon and Google.

6) Business VPN & VoIP Service Providers

Business VPN/VoIP operators are companies that use IP and MPLS transport networks along with specialized network elements to create the higher level services. The business VPN/VoIP operators can either use their own infrastructure, or the transport networks of one or more backbone operators to provide the connectivity for their services. VPN services involve the creation of "private" networks that are isolated at the IP layer but share the same underlying packet transport infrastructure. VoIP services are provided over SIP trunks, to a set of voice processing systems that use IP as a transport mechanism, along with interconnections to other VoIP networks and to the Public Switch Telephone Network (PSTN). The services provided by business VPN/VoIP providers are virtual private networks and voice SIP trunks to enterprises or other service providers. The VPNs and SIP trunks may be isolated, or may connect to the Internet or other VPNs over carefully controlled interconnections through Session Border Controllers (SBCs). The voice services can include internet voice services for a company as well as interconnection to the PSTN and long distance services. Examples of Business VPN/VoIP operators are XO Communications, 8X8, Vonage and Masergy Communications.

7) Cloud (XaaS) Operators

Cloud (XaaS) Operators refer to companies providing an increasing number of IT functions that physically resides in a data center and are delivered over the Internet to the end user, rather than provided locally or on-site as a service. Cloud operators create, maintain and scale computing solutions like CPU capacity, memory storage, and database infrastructure for customers. All service management, software

[71] See Pathan, A. and Buyya, R., Grid Computing and Distributed Systems Laboratory, *A Taxonomy and Survey of Content Delivery Networks* (2007), *available at* http://www.cloudbus.org/reports/CDN-Taxonomy.pdf.

updates, resource replacement, and scaling is done remotely, typically implemented with large homogeneous data centers with virtual servers and virtual networks. There are numerous types of Cloud (Xaas) Operators:

i. ***Software as a Service (SaaS) Operators*** are companies that, through software licensing and a delivery model which is centrally hosted. SaaS Operators provide many business applications (office & messaging software, management software, computer-aided design [CAD] software, accounting software, customer relationship management [CRM] software, etc.) to end users. Examples of SaaS providers include Microsoft 365, Cisco WebEx, and Salesforce.

ii. ***Infrastructure as a Service (IaaS) Operators*** are companies that allow an organization outsource equipment to that owned by the IaaS operator to support operations, including storage, hardware, servers and networking components based on the consumption of the user. Examples of IaaS operators include Amazon Web Service (AWS), Microsoft Azure, and Google Compute Engine (GCE).

iii. ***Platform as a Service (PaaS) Operators*** provide cloud components to end users' software, providing a framework the end user can build upon to develop or customize applications. PaaS operators aim to make the development, testing, and deployment of applications more efficient and cost-effective. Examples of PaaS operators include Apprenda, LongJump, and IBM SmartCloud.

iv. ***Network as a Service (NaaS) Operators*** provide a service in which the capability provided to the cloud service customer is transport, connectivity and related network capabilities. An example of a NaaS provider is Level3 Communications.

v. ***Cloud Real Estate Investment Trusts (REITs)*** are companies that build out physical data center resources like buildings, commercial and backup power plants, fuel generators, fiber connectivity and in most cases equipment racks. Once they build out this data center infrastructure, they then can lease these resources to customers who wish to rapidly deploy their cloud services and do not wish to invest in the physical plant of a cloud data center. Examples of Cloud Real Estate Investment Trusts (REITs) are Digital Realty Trust, Equinix, Dupont-Fabros, and RackSpace.

8) Over-The-Top (OTT) Service Providers

Over-The-Top (OTT) Service Providers are service providers that provide end user access to audio, video, and other content over the Internet rather than via a service provider's own dedicated, managed network. OTT service providers deliver content directly from content producer to the end user using an Internet connection, independent of the end user's ISP and without any infrastructure investment on the part of the provider.

i. ***OTT Video Streaming Service Providers*** are companies that provide video content to end users using the OTT model. Examples of OTT video streaming service providers include Netflix, Hulu, and Crackle.

ii. ***OTT Television On-Demand Service Providers*** are companies that provide television content at the time preferred by the end user ("on demand") using the OTT model. OTT television on-demand systems can either stream content through a set-top box, a computer or other device, allowing viewing in real time, or download it to a device such as a computer, digital video recorder (also called a personal video recorder) or portable media player for viewing at any time. Examples of OTT television on-demand service providers include Apple, Google, NBC On Demand and CBS On Demand.

iii. ***OTT VoIP Service Providers*** are providers of voice services using the OTT model. These services allow for a user to avoid paying for the dedicated phone line as is the case with traditional telephony, and relies on the underlying service provider's connection to the Internet. Examples of OTT VoIP Service Providers include Vonage, Skype, Viber, and MagicJack.

9) Online Content Producers/Distributors

Online Content Producers/ Distributors are organizations that create, edit and arrange text, video, audio, images and other materials that may be included in an Internet-based forum.

i. ***Video Producers*** are entities that create video by capturing moving images, and creating combinations and reductions of parts of this video in live production and post-production. Examples of video producers include 20th Century Fox and Dreamworks. Once video content is compiled, it can be offered to the public via content distributors like broadcast networks, cable networks, and over the top players like Netflix and Google's YouTube.

ii. ***Photograph Producers*** are entities that create photographs, and create photography content through image manipulation. Once the photographers produce their photographic files, they can sell them or offer them via Photo distributors. Examples of photo distributors include iStock Photo and Shutterstock.

iii. ***Blogs*** are websites or web pages on which an individual record opinions, link to other sites, etc., on a regular basis.

10) Applications Producers/Distributors

Application Developers are people, companies and entities that write computer programs to meet specific requirements, including the determination of requirements as well as testing of the software application. Applications enable features and services for devices across the consumer and business sectors. Examples of application developers of all sizes, from all over the world. Application developers can range from companies like IBM to two kids in a garage.

Application Distributors are entities that allow end users to peruse and download applications, whether at no cost or for a fee. Examples of application distributors include Sourceforge, Apple's App Store and Google Play.

11) Hardware/Software/OS/CPE Vendors

Backbone & Access Hardware Systems: Vendors supply the HW/SW/OS that are the critical components of the communications industry. These components are typically located on carrier premises, customer (enterprise/residential) premises, cloud/ data centers, or any combination. They include user devices, Network Access systems, Controllers, Switching, Signaling and Routing Systems, applications to invoke services. In addition to the hardware components, the vendors also offer systems that are capable of monitoring network fault conditions, configuration management, device management (e.g.,. MDM), security and performance. The applications and software is developed open as well proprietary software and hardware systems in compliance with industry standards and best practices. The trend is to use virtualization for systems as well security applications. These components typically have built-in fundamental security capabilities such as authentication, encryption, and packet filtering on the bearer, control and management interfaces and also provide security logging for downstream processing. Due to the complexity of network solutions many vendors offer managed security services to their customers. Examples of hardware vendors include Alcatel-Lucent, Juniper, Cisco, and Adtran.

Operating System Vendors are entities that provide software that manages computer hardware and software resources to end users. This software provides common services for computer programs and allows applications a platform on which to function. Examples of operating system vendors include Microsoft (Windows), Apple(OSX/IoS) and Google(Android).

Browser Vendors are entities that provide software programs used to navigate the Internet with a graphical user interface for display of HTML files. Browsers allow end users to retrieve, present and traverse web pages, images, videos or other pieces of content on the Internet. Examples of browser vendors include Mozilla(FireFox), Microsoft(Windows), Apple(Safari), and Google(Chrome).

12) eCommerce Companies

eCommerce Companies are companies which conduct commerce by way of the Internet or other electronic networks. The widespread use of the Internet, access to

new sales channels have greatly benefitted both to traditional "brick and mortar" establishments as well as new online retailers. Notable examples of eCommerce companies include eBay, Craigslist, and Amazon.

13) Edge Device Companies (Smartphones, Tablets, IoT gadgets)

Edge device companies are companies which produce devices that reside on the periphery of an enterprise or service provider network, providing entry points into these networks. Examples of these devices range from a laptop, smartphone, tablet, smart meter, router, etc. Examples of edge device companies include Apple, Samsung, Nokia and LG.

14) Social Media Companies

Social Media Companies are companies that provide applications which enable users to create and share content, or to participate in the creation and exchange of, user-generated content. Examples of social media companies include Facebook, LinkedIn, and Pinterest.

15) Internet Service Infrastructure Clearinghouses

Infrastructure Clearinghouses are companies that perform an intermediary function between service providers and a large group of end users. These clearinghouses usually perform functions that are vital to the business success of many smaller sized companies that cannot afford the massive investment to perform these functions themselves. An example of this is Intrado. They connect numerous small telecom companies to an ability to route E911 calls to the correct Public Serving Access Point (PSAP). Rather than buy and build numerous dedicated selective routers for E911 calls, these smaller Telecom companies can purchase this function from Intrado. Intrado already has built out the connectivity to the PSAPs, so when these smaller Telecom companies connect to Intrado, they can reach the necessary PSAPs that will serve their customers. Verisign performs DNS queries and responses necessary to enable end users to find websites on the Internet. Neustar operates numbering databases that supports the North American Numbering Plan. They also run various DNS operations to enable the various functions of the Internet to work. These clearinghouses offer unique functions and services at a wholesale level and provide vital services that communications providers need to fulfill their business models. As previously mentioned, examples of these Infrastructure Clearinghouses include Verisign, Neustar, Intrado, iconnectiv, and the Internet Society.

16) End Users (Consumers, Enterprise, Governments)

End Users are the ultimate consumers of any final product or service, regardless of their segment or purpose. For example, this category includes but is not limited to private consumers, enterprise users, and government users.

17) Relay Service Providers

A Relay Service Provider is an operator that allows end users with auditory or visual definitions. These services take place through a variety of platforms, such as text relays through instant messaging, websites, TTYs, or video relays through videophones. These services are subsidized by the FCC's Telecommunications Relay Service (TRS) Fund. Relay service providers can be divided into two categories:

i. ***Telecommunications Relay Service Providers*** are entities who are deaf, hard-of-hearing, deaf-blind, or have a speech disorder to place calls to standard telephone users via a keyboard or assistive device. Relay services typically are enabled real-time text capable technology such as a personal computer, laptop, mobile phone, PDA, and many other devices. Examples of relay service providers include Purple Communications and Sorenson.
ii. ***Video Relay Service (VRS) Providers*** enable persons with hearing disabilities who use American Sign Language (ASL) to communicate with voice telephone users through video equipment, rather than through typed text. Video equipment links the VRS user with a TRS operator – called a "communications assistant" (CA) – so that the VRS user and the CA can see and communicate with each other in signed conversation. Examples of VRS Service Providers include

18) Security Vendors

Anti-virus Software Vendors are entities that provide computer software used to prevent, detect and remove malicious computer viruses. Anti-virus software works against other types of malware, such as backdoors, trojan horses, worms, adware, and spyware. Examples of Anti-virus software vendors include McAfee and Symantec.

Firewalls & Security Appliance Vendors are entities that provide software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network that is not assumed to be secure and trusted. Examples of firewall vendors include Cisco Systems and Juniper Networks.

Intrusion Detection/Deep Packet Inspection Vendors are entities that provide computer software or hardware that enables network packet filtering of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. This software enables advanced network management, user service,

and security functions. Examples of intrusion detection/deep packet inspection vendors include Ericsson and Nokia Siemens Networks.

19) International Service Providers

Global Network Operators

A Global Network Operator is an organization which offers network services across borders. Global Network Operators provide the means for connectivity on a global basis in both wireless and wired space. Examples of Global Network Operators include Deutsche Telekom, TATA Communications, and Nippon Telegraph and Telephone Corporation (NTT).

Global Content Producers

A Global Content Producer is an organization which provides services in the form of content to end users over the Internet of Things (IoT) or a CDN. Examples of Global Content Providers include Comcast, Walt Disney, and Time Warner, Yahoo and Google.

20) Research Institutions

Think Tanks are organizations that perform research and advocacy concerning any topic of interest. Think tanks may be non- or for-profit, and may be funded by private and/or government entities. Examples of think tanks include the Information Technology & Innovation Foundation and the Technology Policy Institute.

Academia is the community of students and scholars engaged in higher education and research within the university education system. Academia is non-profit, and may be funded by private and/or government entities. Examples of academia are the University of Virginia and the Illinois Institute of Technology.

Associations are typically nonprofit organizations formed around a particular profession, the interests of individuals engaged in that profession, and the public interest. Associations engage other stakeholders (government or private) on behalf of their membership across contexts. Examples of associations include the Internet Association, CTIA – The Wireless Association, The Telecommunication Industry Association-TIA, National Cable TV Association –NCTA, the National Telecommunications Cooperative Association-NTCA and the US Telecom Association.

21) Regulators

A regulatory agency is a government agency that regulates businesses in the public interest. An independent regulatory agency operates independent of the Executive Branch/President and is typically established by the Congress. Regulators can be Federal, State, Local, as well as International.

- ***Federal*** Federal Regulators are United States executive branch departments and agencies or independent departments and agencies having responsibility for developing and enforcing rules and regulations in accordance with the Code of

Federal Regulations (CFR).[72] Title 47 of the CFR addresses the Telecommunications federal rules and regulations. It assigns telecommunications regulatory responsibilities to the Federal Communications Commission,[73] Office of Science and Technology Policy,[74] National Security Council,[75] National Telecommunications and Information Administration[76] (Department of Commerce), and the National Highway Traffic Safety Administration[77] (Department of Transportation).

- ***State*** State Regulators are regulators having responsibility for developing and enforcing rules and regulations within their states (i.e., intrastate jurisdiction). For telecommunications, the primary state regulator is often the state's public utility commission.[78] One of the functions of State Regulators is to approve/disapprove the rates (known as tariffs) charged by the utilities for which they regulate.
- ***Local*** Local Regulators are regulators having responsibility for developing and enforcing rules and regulations within a city, county, or other limited geographical region (e.g., municipalities). Local regulators typically regulate cable TV franchises and local public safety communications. Examples include the Fairfax, Virginia department of cable and consumer services[79] and the Fairfax Planning Commission.[80]

22) Public Safety Networks

Broadly defined, the public safety community performs emergency first-response missions to protect life, health, property, natural resources and to serve the public welfare. Public safety operations require effective command, control, coordination, communication, and information sharing tools to support law enforcement, firefighting operations, emergency medicine, search and rescue, and other critical response services. A public safety network is an interagency collaboration capability focused on the development and use of information and communication technologies (ICT) to support information sharing and communications interoperability needs of public safety organizations.

- ***Land Mobile Radio (LMR)***: Public safety personnel have unique communications requirements, which differ from those typically provided commercially because of

[72] *See* 47 C.F.R.
[73] *See id*. at §§ 0 - 199.
[74] *See id*. at §§ 200 - 299.
[75] *See id*.
[76] *See id*. at §§ 300 - 399.
[77] *See id*. at §§ 400 - 499.
[78] *See* Federal Communications Commission, *State Public Utility Commission Contact List*, http://transition.fcc.gov/wcb/iatd/state_puc.html (last visited Mar. 13, 2015).
[79] *See* Fairfax County Virginia, *Department of Cable and Consumer Services*, http://www.fairfaxcounty.gov/dccs/ (last visited Mar. 13, 2015).
[80] *See* Federal Communications Commission, *Planning Commission*, http://www.fairfaxcounty.gov/planning/ (last visited Mar. 13, 2015).

their direct role in saving lives, preventing injury, and limiting property loss. Public safety users currently rely on LMR systems to support mission critical wireless requirements.

- ***Next Generation 911 (NG 911):*** NG911 is an Internet Protocol (IP) based system comprised of managed Emergency Services IP networks (ESInets), functional elements (applications), and databases that replicate traditional E911 features and functions and provides additional capabilities. NG911 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety Answering Points (PSAPs) and other emergency service organizations.[81] Examples of NG911 providers include Intrado and TeleCommunications System (TCS).
- ***Emergency Services IP Network (ESINet):*** An ESInet is a managed Internet Protocol (IP) network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG911 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks). Examples of ESINet providers include Intrado and TeleCommunications System (TCS).
- ***FirstNET:*** The need to access and share information is driving investments in new wireless networks. A nationwide public safety wireless broadband network (FirstNET) promises to enable solutions that will add broadband data to emergency responder communications. FirstNet will create a nationwide, standardized, network with dedicated spectrum to provide public safety access to advanced broadband communications. Once fully developed, FirstNet will enable public safety communications to leverage commercial broadband standards, technologies, devices and will connect to commercial networks and the Internet.

23) Standards Bodies

No single organization defines the standards for the Internet. The standards for the Internet are developed through the collaboration of multiple standards organizations and industry working groups. Standards organizations and industry working groups that contribute to the development of cybersecurity and network security standards include:

- ***Internet Engineering Task Force (IETF)***: The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the

[81] *See* National Emergency Numbering Association, *What Is NG9-1-1?* (2008), *available at* http://www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf.

smooth operation of the Internet.[82] The IETF provides standards for Internet protocols and how to secure them. Examples include IPSEC, BGPSec, SSL, DNSSec, and TLS.

- ***Metro Ethernet Forum (MEF):*** The MEF, as the defining body for Carrier Ethernet, is a global industry alliance comprising more than 220 organizations including telecommunications service providers, cable MSOs, network equipment/software manufacturers, semiconductors vendors and testing organizations.[83] MEF develops the standards for Carrier Ethernet and as part of developing those standards works to make them secure.
- ***Alliance for Telecommunications Industry Solutions (ATIS):*** ATIS is a standard development organization that develops technical and operational standards and solutions for the ICT industry. ATIS is accredited by the American National Standards Institute (ANSI).[84] ATIS creates standards for the information, entertainment, and communications marketplace, and as part of developing these standards it also works to make them secure.
- ***Telecommunications Industry Association (TIA):*** TIA is a trade association representing the global information and communications technology (ICT) industry through standards development and policy initiatives. TIA develops standards in the telecommunications industry, and is accredited by ANSI.[85]
- ***ITU: ITU (International Telecommunication Union)*** is the United Nations specialized agency for information and communication technologies. The ITU allocates global radio spectrum and satellite orbits, develops technical standards, and makes efforts to improve access to ICTs to underserved communities worldwide.[86] The ITU develops recommendations that are used by the telecommunications industry. Included in those recommendations are security recommendations.
- ***ICANN:*** ICANN is a not-for-profit public-benefit corporation that develops policy on the Internet's unique identifiers through its coordination role of the Internet's naming system.[87]
- ***Society of Cable Telecommunications Engineers (SCTE):*** the SCTE develops technical specifications for the cable telecommunications industry and provides technical specifications for securing cable networks. Examples include DOCSIS' Baseline Privacy specification.[88]

[82] *See* The Internet Engineering Task Force, http://www.ietf.org/ (last visited Mar. 13, 2015).
[83] *See* Metro Ethernet Forum, http://metroethernetforum.org/ (last visited Mar. 12, 2015).
[84] *See* Alliance for Telecommunications Industry Solutions, http://www.atis.org/ (last visited Mar. 12, 2015).
[85] *See* Telecommunications Industry Association, http://tiaonline.org/ (last visited Mar. 12, 2015).
[86] *See* International Telecommunication Union, http://www.itu.int/en/Pages/default.aspx (last visited Mar. 12, 2015).
[87] *See* Internet Corporation for Assigned Names and Numbers, https://www.icann.org/ (last visited Mar. 12, 2015).
[88] *See* Society of Cable Telecommunications Engineers, http://www.scte.org/ (last visited Mar. 12, 2015).

- ***European Telecommunications Standards Institute (ETSI)***: ETSI develops telecommunications standards for the European market and developed the Global System for Mobile Communications (GSM) standard that has since evolved to Long Term Evolution (LTE) standard through the 3rd Generation Partnership project (3GPP). As part of developing the mobile communications standards, they include standard for securing them.[89]
- ***World Wide Web Consortium (W3C):*** The W3C develops the Web standards used by browsers. The W3C addresses security as part of developing the standards. Examples of this include HTTPS.[90]
- ***Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG):*** MAAWG is an industry group that develops initiatives in three areas to resolve abuse problems: industry collaboration, technology, and public policy. MAAWG has brought together experts to help develop solutions to email abuse (SPAM), malware (i.e. Botnets), and robo-calling (voip SPAM).[91]

24) 'Exploit' Websites

Hackers are persons that utilize the Internet to gain unauthorized access to data, database and computing systems, and either steal, destroy or corrupt these entities. Hackers may utilize a wide array of vectors to attain unauthorized access. One such Ecosystem category that is used extensively by hackers is Exploit websites. Once a hacker has learned a specific vulnerability, a weak point of entrance or a process that will harm a specific Internet entity, it will post what it has learned onto various 'Dark' websites in an effort to encourage others to follow and repeat their actions. Hacktivists like Lulsec or Anonymous are persons that utilize the Internet to further political or social purposes. They are extensive users of these types Exploit websites.

25) Public/Private Power Utilities

Electric Power Utilities generate, transmit, and distribute electric power necessary for operating communications sector's systems and networks. Communications sector systems and networks cannot operate without electric power, therefore electric utilities provide a critical capability and all players in the communications sector are critically dependent on electric utilities. Water utilities provide safe drinking water to the general public and businesses. Gas and oil utilities provide energy for heating to the general public and business.

Utilities may be owned by a variety of entities, including:

- Investor-Owned Utilities (IOU) e.g., Duke Energy, Pepco Holdings, Exelon, and Pacific Gas and Electric (PG&E)
- Cooperatives e.g., Great River Energy (GRE), Tri-State, Brunswick

[89] *See* European Telecommunications Standards Institute, http://www.etsi.org/ (last visited Mar. 13, 2015).
[90] *See* The World Wide Consortium, http://www.w3.org/ (last visited Mar. 13, 2015).
[91] *See* Messaging, Malware and Mobile Anti-Abuse Working Group ('M3AAWG'), https://www.m3aawg.org/ (last visited Mar. 13, 2015).

- Municipally-owned, e.g. Los Angeles Department of Water and Power (LADWP), Nashville Electric Service (NES), or Santee Cooper
- Government-owned entities, e.g., Tennessee Valley Authority (TVA) and Bonneville Power
- Utilities frequently combine a variety of services, with many companies providing water and gas, electric and water, or electric and gas.
- Utilities also deploy and manage private communications networks and therefore are members of the communications sector. Many utilities operate their own wired and wireless backbones (Backbone Operator). Furthermore, in rural communities some utilities provide broadband and ISP services to local private customers (ISP). Utilities may run their billing systems (eCommerce), and operate their VPNs and VoIP networks. Utilities also may be buying these services from the communications sector companies and are therefore represented in the End User/Consumer/Enterprise category.
- Utility Company size and sophistication vary greatly, from large Fortune 500 companies to relatively small cooperatives with approximately 140 employees and possibly fewer. Examples of various sized power utilities are Consolidated Edison-ConEd, National Grid, PEPCO, and Duke Energy.

Smart Grid generally refers to a class of technologies that use computer-based remote control and automation of electrical power distribution. These systems are made possible by two-way communication technology and automated processing that can monitor and control the power grid network as well as individual power feeds into homes, office building and industrial locations. Smart Grids offer many benefits to utilities and consumers -- mostly seen in big improvements in energy efficiency on the electricity grid and in the energy users' homes and offices. The "grid" amounts to the networks that carry electricity from the plants where it is generated to consumers. The grid includes wires, substations, transformers, switches and much more.

Much in the way that a "smart" phone these days means a phone with a computer in it, smart grid means "computerizing" the electric utility grid. It includes adding two-way digital communication technology to devices associated with the grid. Each device on the network can be given sensors to gather data (power meters, voltage sensors, fault detectors, etc.), plus two-way digital communication between the device in the field and the utility's network operations center. A key feature of the smart grid is automation technology that lets the utility adjust and control each individual device or millions of devices from a central location.

Most of the traditional power distribution grid is built using a "hub-and-spoke" pattern. The Smart Grid can connect the "spokes" to enable multiple distribution paths. When facing an issue like a tree falling on a line, a lightning strike, or a short circuit, Smart Grid technologies collectively called "distribution automation" can sense the problem and automatically reroute power around it.

Smart Meters are devices that make it easy for utilities—and consumers —to obtain accurate, real-time readings of electricity usage. With smart meter data, utilities can manage power distribution more efficiently to avoid overloading to the grid and the blackouts that follow.

The reason Smart Grids are an important piece of the Ecosystem is that many utility companies are building IP-based communications networks to support the Smart Grid command and control and some are actually connected to and rely on the Internet. Although with growing security concerns, many of the IP-based Smart Grid networks are going back to being separated from the public Internet and may connect to a next generation industrial Internet network.

26) Open Source Community

Open Source Software/Systems are software and systems based on source code which is not restricted from viewing, modifying, or transferring by license (however such license may protect the integrity of the source code). Such software and systems may be developed by a volunteer or corporate-backed community, or commercially. Examples of Open Source Software/Systems include Android, Ubuntu, and Linux.

Open Source Applications are applications built from open source code and which are not restricted from viewing, modifying, or transferring by license. Such applications may be developed by a volunteer or corporate-backed community, or commercially. Examples of Open Source Applications include Mozilla Firefox, Apache/Tomcat, Asterisk, MySQL and NASA World Wind.

Open Source Sandboxes are repositories for source code repositories for open source software development. The repositories typically offer free access to hosting and tools for developers of open source software. Examples include Sourceforge.net and GitHub.com

27) Electronic Payment Service Providers

Electronic Payment service providers include the major credit card companies and their associated communications networks that enable an end user to swipe their credit and debit cards when making purchases and returns an authorization for their requested purchases. These electronic payment transactions take place over what is called the electronic payment system. The electronic payment system is an operational network - governed by laws, rules and standards - that links bank accounts and provides the functionality for monetary exchange using bank deposits. The payment system is the infrastructure (consisting of institutions, instruments, rules, procedures, standards, and technical means) established to affect the transfer of monetary value between parties discharging mutual obligations. Its technical efficiency determines the efficiency with which transaction money is used in the economy, and risk associated with its use. A large number of electronic payment systems have emerged. These include debit cards, credit cards, electronic funds

transfers, direct credits, direct debits, internet banking and e-commerce payment systems.

Payment systems may be physical or electronic and each has its own procedures and protocols. Standardization has allowed some of these systems and networks to grow to a global scale, but there are still many country- and product-specific systems. Examples of payment systems that have become globally available are credit card and automated teller machine networks. Specific forms of payment systems are also used to settle financial transactions for products in the equity markets, bond markets, currency markets, futures markets, derivatives markets, and options markets, and to transfer funds between financial institutions both domestically using clearing and Real Time Gross Settlement (RTGS) systems and internationally using the SWIFT network.

Electronic verification systems allow merchants to verify in a few seconds that the card is valid and the cardholder has sufficient credit to cover the purchase, allowing the verification to happen at time of purchase. The verification is performed using a credit card payment terminal or point-of-sale (POS) system with a communications link to the merchant's acquiring bank. Data from the card is obtained from a magnetic stripe or chip on the card; the latter system is called Chip and PIN in the United Kingdom and Ireland, and is implemented as an EMV card.

Point-of-Sale (POS) Networks is the place where a retail transaction is completed. It is the point at which a customer makes a payment to the merchant in exchange for goods or services. At the point of sale the retailer would calculate the amount owed by the customer and provide options for the customer to make payment. The merchant will also normally issue a receipt for the transaction. The POS in various retail industries uses customized hardware and software as per their requirements. Retailers may utilize weighing scales, scanners, electronic and manual cash registers, EFTPOS terminals, touch screens and any other wide variety of hardware and software available for use with POS.

Payment System /Telecom Partnerships: Several Telecom companies have partnered with several credit card companies to build the next generation of POS and payment networks. The next generation POS system is based on near field communication (NFC) and allows users to pay by tapping their mobile device to a payment terminal. This new mobile electronic payment consortium has initially partnered with the Discover network and Barclaycard US. In July of 2011, a partnership was announced between this mobile electronic payment consortium and Visa, MasterCard, Discover, and American Express. Also in 2011 the three largest wireless carriers Verizon, AT&T and T-Mobile, announced plans to invest in this next generation electronic payment network.

9.8 MEASUREMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY

This report outlines the analysis and findings of the Measurements Working Group within CSRIC Working Group 4. The objectives of the working group were to provide insight into what constitutes meaningful indicators (i.e., cybersecurity metric(s)) of successful cybersecurity risk management; facilitate communication regarding the cybersecurity metrics among Internet Service Providers (ISPs); and suggest practices that companies may consider in the development and incorporation of metrics into their internal cybersecurity programs.

The Measurement Working Group's analysis indicates the following actions to fulfill the Working Group's goals: 1) develop a process for industry and government engagement to discuss meaningful indicators of cybersecurity risk management led by a standing review group under the Communications Sector Coordinating Council[92] (CSCC), and 2) propose quantitative measures and qualitative examples that the CSCC could include in its Sector Annual Report[93] (SAR), to provide comprehensive analysis of the existing state of the critical communications infrastructure.

Members of the Measurements Working Group agreed that their scope of work would center on the development of measures associated with ensuring the availability, reliability, resiliency, and integrity of communications critical infrastructure, consistent with the national performance goals recommended by the Department of Homeland Security (DHS) during its implementation of Executive Order 13636.[94] In addition, the Working Group adopted the definition of "critical infrastructure" that is contained in Executive Order 13636, which identifies critical infrastructure based upon a catastrophic standard.[95]

This report provides a brief background on cybersecurity metrics based on existing industry standards and guidelines and outlines steps for developing cybersecurity metrics that companies may incorporate into their cybersecurity risk management programs. The report also discusses the challenges in developing cybersecurity metrics. Those challenges include correlating cyber threats to any specific industry sector and difficulty establishing a correlation between any specific cybersecurity practice and a cybersecurity outcome.

Finally, the report concludes by identifying high level metrics that the CSCC, in partnership with DHS and Federal Communications Commission (FCC), could take under consideration for inclusion in the SAR to help provide macro level information on the state of cybersecurity for

[92] *See* Communications Sector Coordinating Council, http://www.commscc.org/ (last visited Mar. 13, 2015).
[93] *See* 2014 CSCC Working Groups, Plans and Reports, *available at* http://www.commscc.org/about/working-groups/.
[94] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013) [hereinafter *EO 13636*].
[95] *Id*. at §9 ("[t]he Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security").

critical communications infrastructure and meaningful indicators of successful cyber risk management for that infrastructure. This information would be reported on an aggregate sector, not company specific, level. The Working Group also finds that in the event the FCC desires more specific information from individual companies, the Working Group recommends that the FCC, in coordination and in conjunction with DHS, develop a voluntary program for annual meetings between the FCC, DHS and individual companies that agree to participate. Companies that choose to participate in this program should be afforded the protections that are already provided by the federal government to critical infrastructure under the Protected Critical Infrastructure Information (PCII) program or a legally sustainable equivalent.

II. FEEDER GROUP STRUCTURE

Chris Boyer – Co-Chair	AT&T
Chris Roosenraad – Co-Chair	Time Warner Cable
Nadya Bartol	UTC
Stacy Hartman	Centurylink
Robert Mayer	USTelecom
Paul Diamond	Centurylink
Ramesh Sepehrrad	Comcast
Matt Tooley	NCTA
Vern Mosley	FCC
Jared Allison	Verizon
Matt Carothers	Cox

III. OBJECTIVE

The purpose of the Measurement Working Group within CSRIC Working Group #4 is to offer analysis and findings regarding meaningful indicators of successful (and unsuccessful) cyber risk management that demonstrate how communications providers are managing cybersecurity risk through the application of the NIST Cybersecurity Framework (or an equivalent construct). The objectives of this group within CSRIC Working Group #4 are as follows:

- To provide insight and criteria on what constitutes a meaningful cybersecurity metric that can serve to inform future discussions about metrics within the Sector and with the FCC.

- To identify processes or standard practices companies may consider building into their risk management programs to assist in informing senior management on how their company is managing cyber risks to their core business.

- To identify a standard process through which the FCC or other government agencies can engage with the sector to meaningfully assess the communication sector's progress towards managing cybersecurity risk.

- To identify measures that the sector has determined best demonstrate the overall availability, reliability, resiliency, and integrity of critical communications infrastructure, as meaningful indicators of successful cyber risk management, that could be included in future drafts of the Sector Annual Report (SAR) starting in 2015. The SAR would be provided to the Department of Homeland Security (DHS), as the Communications Sector Specific Agency (SSA), and the Government Coordinating Council (GCC) which includes the FCC, to provide visibility into progress within the communications sector based on the cybersecurity metrics.

****** Due to a variety of factors, particularly those outlined in Section IV, the Working Group has concluded that it is very difficult to measure security and to establish a cause for any particular cyber practice. For this reason the findings outlined in this Appendix are focused on measuring communication sector collective outcomes as opposed to individual company best practices. Further, many cyber threats span industries and thus cannot be easily correlated back to any one entity. Therefore, the Working Group focused its analysis on communications critical infrastructure managed by communications network service providers.

IV. SCOPE AND AUDIENCE

The scope for this work is focused upon measures[96] associated with ensuring the availability, reliability, resiliency and integrity of communications critical infrastructure, as meaningful indicators of successful cyber risk management, consistent with the national performance goals recommended by DHS in implementing Executive Order 13636.

For the purposes of this report, critical infrastructure is defined as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[97] For example, as outlined in the wireline subgroup report, the critical infrastructure considered by the subgroup included the core communications networks such as the network backplane and critical services. As such, this report is focused upon measurements or measures related to ensuring the availability, reliability, resiliency and integrity of each segment's critical infrastructure with their respective communications networks.

The group focused on meaningful indicators of successful cyber risk management and did not focus on measurements related to cybersecurity writ large given the difficulty in correlating cybersecurity issues back to specific ISP actions. There are some potential data points that may be relevant to evaluating cybersecurity across the board such as infection rates and other data.

[96] For the purpose of this document the terms "measure" and "metric" are synonymous. This report uses the term "measure" because this term is used in international standards on security measurement and system and software measurement. However, it should be noted that the term "metric" as used by NIST means the same as "measure" when used by ISO. ISO/IEC 27004, Information Security Management System Measurement Defines "measure" as "variable to which a value is assigned as the result of measurement" where "measurement" is the process of obtaining information that makes up a measure.

[97] *EO 13636* at §9.

However, these data points are more relevant to the entire ecosystem. Therefore, the data points should be considered as part of a cross-ecosystem analysis rather than addressed in isolation within CSRIC, which is unique to ISPs. The ecosystem analysis is being contemplated by the Department of Commerce and NIST as a result of their recent Request for Information (RFI) on the use of the framework.[98]

This work is focused on potential macro-level practices and measures that may be considered by firms for use by senior executives to allow meaningful assessments to be made both internally (e.g., Chief Security Officers and senior corporate management) and externally (e.g., business partners). The objective is to develop data points that are actionable, simple to understand, relevant, and related solely to the four objectives outlined above. This document is not intended to be proscriptive in nature or become a "checklist" of measures. Moreover, this document does not provide specific descriptions of existing measurement methodologies or identify an exhaustive list of cybersecurity measures. The measures outlined are the result of the measurements working group's analysis and findings that the CSCC could take under consideration in preparing the annual SAR.

The following national and international standards, guidelines, and best practice documents were consulted in the development of this document:

- NIST 800-55 Rev1 - *Performance Measurement Guide for Information Security*[99]
- ISO/IEC 27004 – *Information Technology – Security Techniques – Information Security Management – Measurement Process*[100]
- ISO/IEC 15939 – *Information Technology – System and Software Engineering – Measurement*[101]
- *Draft Practical Measurement Framework for Software Assurance and Information Security*[102]

[98] *See* National Institute of Standards and Technology, *Experience With the Framework for Improving Critical Infrastructure Cybersecurity*, 79 FR 50891 (Aug. 26, 2014) [hereinafter *NIST RFI*] , *available at* https://www.federalregister.gov/articles/2014/08/26/2014-20315/experience-with-the-framework-for-improving-critical-infrastructure-cybersecurity.

[99] National Institute of Standards and Technology, *Performance Measurement Guide for Information Security* (2008), available at http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[100] International Organization for Standardization, *ISO/IEC 27004:2009* (2013), *available at* https://www.iso.org/obp/ui/#iso:std:42106:en.

[101] International Organization for Standardization, *ISO/IEC 15939:2007* (2012), *available at* http://www.iso.org/iso/catalogue_detail.htm?csnumber=44344.

[102] *See* Practical Software and Systems Management, *Draft - Practical Measurement Framework for Software Assurance and Information Security* (2008), *available at http://www.psmsc.com/Downloads/TechnologyPapers/SwA%20Measurement%2010-08-08.pdf*.

V. WHAT MAKES A GOOD CYBERSECURITY METRIC?

A. BACKGROUND

According to national and international standards and guidelines on security measures/metrics,[103] cybersecurity metrics should be built to support specific performance goals and objectives. For example, the NIST cybersecurity framework contemplates firms determining their core mission, cybersecurity threats or risks to that core mission and then developing a "profile" of internal practices and controls, pulling from the suggested practices in the framework, to best manage those risks. Cybersecurity metrics should support those efforts.

For example, a firm may elect to implement a standard to minimize security threats stating that, "All employees should receive adequate information security awareness training" which is consistent with the recommended prevention practices in the framework. In this example, an appropriate goal may be that "All new employees receive security training on an annual basis." A metric would follow monitoring the accomplishment of the objectives by quantifying the implementation of that particular goal, such as periodic status updates on the percentage of employees trained. These metrics should include enterprise-level guidance and correspond to the operational priorities of the organization.

Examples of information security activities that can provide data for measurement include risk assessments, penetration testing, security assessments, and continuous monitoring. Other assessment activities, such as the effectiveness of a training and awareness program, can also be quantified and used as data sources for measures. Management should use measures to review performance by observing trends, identifying and prioritizing corrective actions, and directing the application of those corrective actions based on risk mitigation factors and available resources. The metrics development process, described below in Section VI, ensures that metrics are developed with the purpose of identifying the cause(s) of poor performance and pointing to appropriate corrective actions. Cybersecurity measures should support the specific performance goals and objectives of an organization.

NIST Special Publication 800-55 Revision 1 identifies the characteristics of good measures that the Working Group recommends should be taken under consideration in determining what constitutes a good cybersecurity metric.

B. ORGANIZATIONAL PRINCIPLES

The following list includes representative principles that organizations may consider in developing internal cybersecurity measurement approaches. These principles should guide

[103] *See* National Institute of Standards and Technology, *supra* note 100, at 361.

an organization as it considers, tailors, introduces, and evolves its cybersecurity measurement activities:[104]

- Security measurement should be integrated into an organization's existing measurement and risk management practices.
- Security measurement should satisfy information needs for a variety of stakeholders/audiences
- Each stakeholder group will generally require tailoring of specific measures based on each group's information needs.
- Different measures targeting different stakeholders may use the same information originating from the same data sources to facilitate multiple uses of the same set of data.
- Security measures should be effective, practical, and worth the investment of resources in the long term.
- Implementation of measurement should incorporate automation to assist analysts in data collection, analysis, and reporting.

For the purposes of this document, the term "measurement" applies to both quantitative and qualitative measurement methodologies. This may also include data that firms obtain from third party data sources who regularly work with firms to provide cybersecurity threat information.

C. WHY IS MEASURING SECURITY DIFFICULT?

Based on practitioner experience in establishing and operating security measurement programs there are several reasons why measuring cybersecurity may be a challenge:

- Cybersecurity is not an exact science and does not provide for exact measurement such as water, temperature, or network throughput. In many cases, it is difficult to determine the success or failure of a given practice, or even if recommended practices are having an impact.
- Inputs, outputs, and outcomes of cybersecurity are separated in time, making authoritative measurement challenging. In other words, protective controls such as security training, access control, or firewalls are believed to work; however, it is very difficult to pinpoint cause and effect. This makes outcomes difficult to articulate and quantify.
- Correlation does not imply causation. For example, the increase in a number of attacks or incidents may simply mean that the intrusion detection and prevention systems have been updated and tuned and are registering a greater number of events which might have gone unnoticed before.

[104] *See* Practical Software and Systems Management, *supra* note 103, at 161 (The principles outlined in this section were adapted from this source).

- Different organizations have different risk environments, goals for cybersecurity, and tools that they use to capture measures, and therefore comparing organizations is challenging and may not be meaningful.

VI. ANALYSIS AND FINDINGS: DEVELOPING RELEVANT MEASURES INSIDE THE FIRM

The following identifies a basic process and considerations regarding how companies could develop internal processes to measure the state of their cybersecurity risk management program. This is not intended to be a checklist or required steps; rather they are actionable steps firms could employ to voluntarily develop the means to measure the state of their cybersecurity programs and be used externally as meaningful indicators of the firm's successful cyber risk management. This process is based on a collective practitioner wisdom that has been codified into numerous standards, guidelines, and best practices over a number of years.[105] Further the Working Group would like to emphasize that implementing a comprehensive cybersecurity program, or making substantial edits to an existing program, takes time as business process have to be developed, tested and implemented. In some cases, new standards or best practices may also need to be developed by standards development organizations.

A. STEPS FOR EVALUATING CYBERSECURITY PROGRAMS WITHIN A FIRM

- Determine the organization's core mission and risks consistent to the process outlined in the NIST cybersecurity framework (e.g., Refer to Wireline subgroup report).
- Determine the organization's specific performance goals and objectives.
- Develop internal controls in support of those objectives.
- Develop methods to evaluate those controls by quantifying the implementation, efficiency, and effectiveness of security controls.
- Collect data to evaluate security controls.
- Analyze collected data and identify possible improvement actions against the performance goals and objectives.
- Document and report cybersecurity progress markers to appropriate stakeholders.
- Use progress markers to support decision making and resource allocation.

[105] *See* Capability Maturity Model Integration Institute, http://cmmiinstitute.com/#home (last visited Mar. 13, 2015) (Capability Maturity Model Integration); *See* National Institute of Standards and Technology, *supra* note 100, at 361; *See* Practical Software and Systems Management, *supra* note 103, at 161; *See* International Organization for Standardization, *supra* note 101, at 361; *See* International Organization for Standardization, *supra* note 100, at 361.

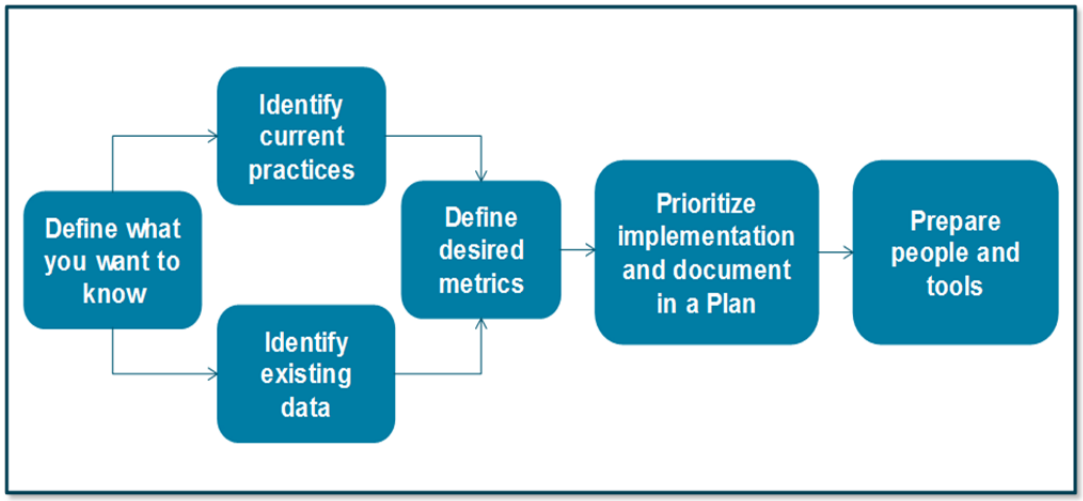
B. CONSIDERATIONS

Users of this document should be aware of important implementation considerations that will assist in making their program a success, including:[106]

- Identify no more than 1 to 3 goals, with associated controls based on current priorities.
- Ensure that the cost of evaluation activities does not exceed the benefit that these activities provide.
- Data quality is important to ensure that any measures are objective and reliable.
- Measures must be useful and relevant
- A measures repository should be utilized to conduct trend analysis that enhances evaluation and effect improvement.
- If measures are not found useful after 2 cycles of use, retire them and identify other measures that can be implemented to gather the same needed information.
- Review, revise, or phase out old measures, and phase in new measures, when targeted level of performance is achieved or when organization's requirements change.
- Measurement should help determine general trends such as improvement or degradation, and help in identifying cause(s) of good or poor performance.
- Information about performance trends and causes of such trends should be used in improvement action and resource allocation decision making.
- Design the measurement program to help motivate desired behavior focusing on improved management and better performance, rather than motivating people to make the numbers look good.
- Use measurement to increase accountability and responsibility and help individuals implement changes required to improve performance, rather than to punish individuals for poor results.
- Identify which measures are to be reported and to who to ensure that only appropriate information reaches each external and internal stakeholder.

[106] These steps are based on Draft Practical Measurement Framework for Software Assurance and Information Security is an industry-developed document that harmonized several measurement methodologies and demonstrated fundamental similarities among them. The industry practitioners who developed this document came from a diverse group of organizations including industry, government, and academia. Many considerations in this list are informed by previously referenced NIST and ISO guidelines and standards.

FIGURE 1: INTERNAL PROCESS FLOW" CREATE/UPDATE MEASURES[107]



VII. ANALYSIS AND FINDINGS: PROCESS TO EVALUATE CYBERSECURITY MEASURES WITHIN THE COMMUNICATIONS SECTOR

A disciplined review process has been identified and could be adopted for future government requests for cybersecurity measurements. To ensure success in providing meaningful measurements, as requested by the FCC, a defined, structured approach should be followed. That structured process should include how to request a potential measurement, how the measurement request will be evaluated for efficacy and finally, submitted for future use.

As contemplated, the Sector process would establish a "front door" for requests. This would relieve the individual CSRIC Working Groups from having to define measures at the same time that the group is tasked to address complex technical and policy issues. A standing review group would be formed with participation from industry experts. Upon request for Industry Measures, the review group would first define/clarify the information sought, and then outline the process that would be undertaken to address the request. The process flow captured in Appendix A will be used as foundation for the framework process definition. The review group would represent industry interests with the goal of responding appropriately to requests for measures. The Measurement Working Group finds that the Communications Sector Coordinating Council (CSCC) can be utilized as that board of review, again, with industry expert participation.

[107] N. Bartol, *Articulating Value of Security Through Cybersecurity Metrics*, presented at EUCI Conference April 2014.

The CSCC would then work with the "Requestor" on individual measures requested; including determining what measures may be effective based on the findings of this CSRIC IV Working Group 4 Measures Working Group. The CSCC will also provide a framework document for the inputs of requests for measures, which will help define the metric being requested and will provide the information required to begin shaping the response. The CSCC will also reach out to standards bodies for input or coordination of efforts as considered necessary. Case Studies and/or longer-term Pilot Programs will be addressed as required to "test" a given metric before recommendations are made on the viability of the metric. Agreed upon Sector measures would then be provided in the Sector Annual Report (SAR) provided to Congress, through the DHS CIPAC process. As a member of the GCC, the FCC would be a participant in the development of this SAR and have access to that information.

Appendix A to this document provides a diagram outlining this proposed process.

VIII. ANALYSIS AND FINDINGS: MEASURES FOR INCLUSION IN SECTOR ANNUAL REPORT (SAR)

An objective of this group is to identify how to best demonstrate the overall state of cybersecurity in terms of meaningful indicators of successful cyber risk management within the communications sector. To accomplish this objective, the Working Group is recommending that the CSCC develop an addendum to the Sector Annual Report (SAR) starting in 2015 to provide meaningful indicators of cyber risk management and the state of cybersecurity in the communications sector. The Working Group is recommending that the SAR include discussion of how cybersecurity risk management processes employed by the sector are addressing the availability, reliability, resiliency and integrity of critical communications network infrastructure.[108] The SAR would then be provided to the Department of Homeland Security (DHS), as the Communications Sector Specific Agency (SSA), and the Government Coordinating Council (GCC), which ensures that the FCC would have visibility into progress within the communications sector.

As noted above, there are numerous challenges associated with cybersecurity metrics given that many data points fall outside ISP's control and are not related to communications critical infrastructure. For this reason, the Working Group focused on quantitative metrics related to the availability, reliability, resiliency and integrity of communications critical network infrastructure which are within ISPs span of control. These quantitative measures can be combined with qualitative examples on major issues and actions that ISPs; for example, the top 3-5 threats faced by industry over a given period of time and use cases or the industry response, to provide a picture of the current threats to critical communications network infrastructure and actions the industry is taking to mitigate those risks.

[108] *See NIST RFI* (SAR may consider questions outlined in the NIST RFI).

IX. SUMMARY FINDINGS

The Measurements Working Group presents its summary findings below. The findings are based on the Working Group's analysis, deliberations, and discussions with leading experts on the subject of meaningful indicators of successful cyber risk management. The summary findings are also consistent with the recommendations noted in the EastWest Institute's "Measuring the Cybersecurity Problem Policy" report.[109] In their report they concluded a trusted private sector entity was needed for cybersecurity metrics and private sector companies should be incentivized to voluntarily contribute data, and subject matter experts should collaborate to develop statistical methods analyzing the data for reporting benchmarks.

- Future requests for metrics by government agencies into the impact of cybersecurity threats to communications infrastructure should be directed to a single point of contact review board within the CSCC which would then analyze the request, along with appropriate subject matter experts, taking in to the consideration the discussion of "good" cybersecurity measures outlined in Section VIII above, to determine if such a metric should be added to the annual SAR.

- Communications network service providers should evaluate how to include metrics into their cyber risk management processes. There are a variety of factors and process steps that firms can consider in developing internal cybersecurity reporting regimes as meaningful indicators of successful cyber risk management to support their overall performance objectives under the NIST Cybersecurity Framework.

- It is difficult to develop cybersecurity measures around the effectiveness of given programs given the cross-sectorial nature of cyber threats. The Working Group finds that more cross-sectorial analysis is needed to determine a comprehensive and valid set of cybersecurity effectiveness metrics. It is inappropriate for those metrics to be completed on an individual sector basis given the difficulty in correlating the threat to one sector. As such, this topic of discussion should continue with DHS as the lead agency responsible for cybersecurity via the CIPAC process.[110]

- The CSCC should work with DHS and the FCC under CIPAC to develop an annual addendum to the SAR that provides both quantitative and qualitative examples of the steps industry is taking to address cyber threats as outlined in Section VIII above. These measures should be high level and at an aggregate level focused on the continuing availability of communications critical infrastructure.

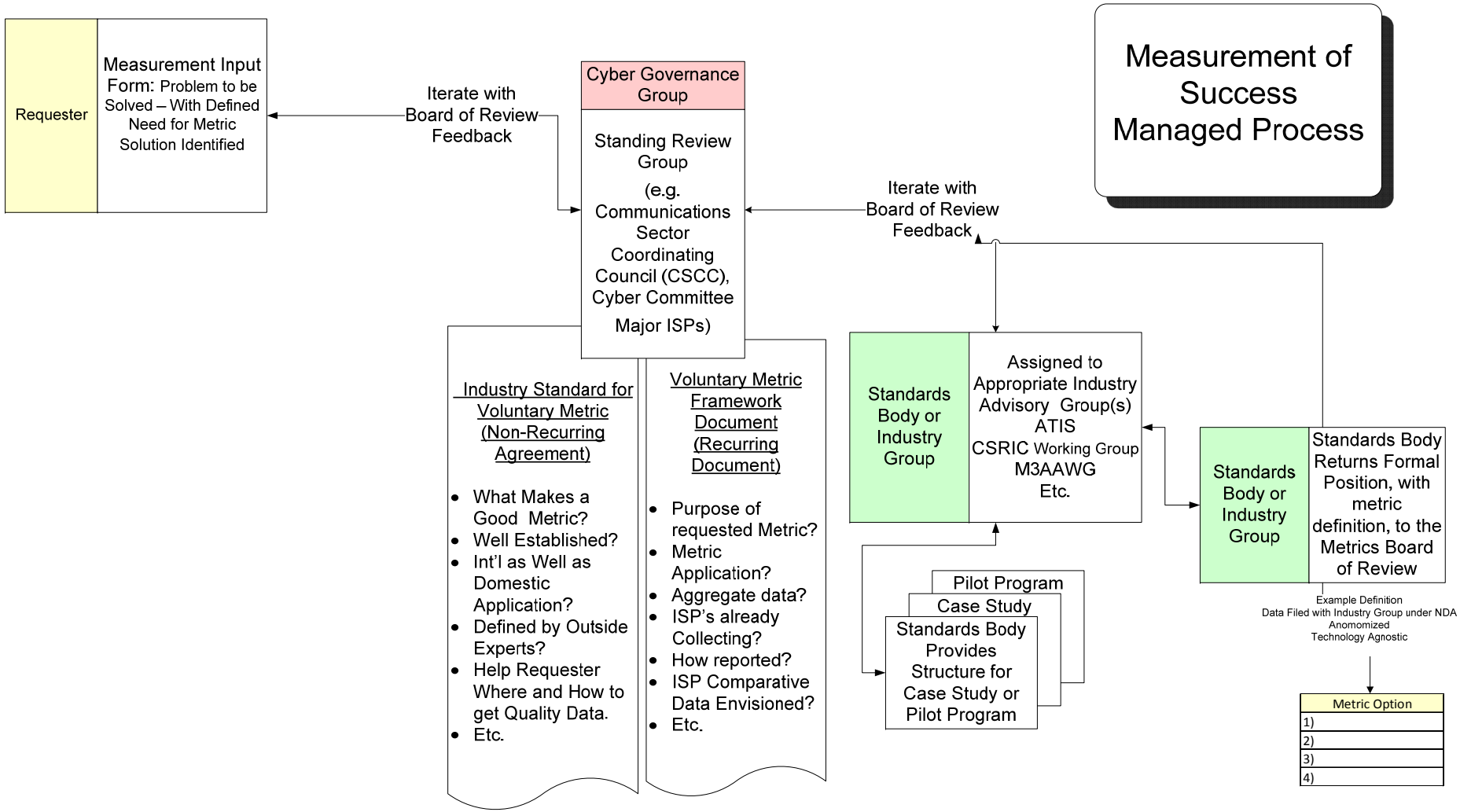
---

[109] *See* EastWest Institute, *Measuring the Cybersecurity Problem* (2013), *available at* http://www.strozfriedberg.com/wp-content/uploads/2013/10/Measuring-The-Cybersecurity-Problem_EWI_ENC_2013.pdf.

[110] *See* Department of Homeland Security, *Critical Infrastructure Partnership Advisory Council*, http://www.dhs.gov/critical-infrastructure-partnership-advisory-council (last visited Mar. 13, 2015) (The DHS Critical Infrastructure Partnership Advisory Council (CIPAC) was established to facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators.)

- In the event the FCC desires more specific information from individual companies, the Working Group recommends that the FCC, in coordination and in conjunction with DHS, develop a voluntary program for annual meetings between the FCC, DHS and individual companies that agree to participate. Companies that choose to participate in this program should be afforded the protections that are already provided by the federal government to critical infrastructure under the PCCII program or a legally sustainable equivalent.

APPENDIX A


Measurement of Success Managed Process
Requester
Measurement Input Form: Problem to be Solved – With Defined Need for Metric Solution Identified
Iterate with Board of Review Feedback
Cyber Governance Group
Standing Review Group
(e.g. Communications Sector Coordinating Council (CSCC), Cyber Committee Major ISPs)
Iterate with Board of Review Feedback
Industry Standard for Voluntary Metric (Non-Recurring Agreement)
What Makes a Good Metric?
Well Established?
Int'l as Well as Domestic Application?
Defined by Outside Experts?
Help Requester Where and How to get Quality Data.
Etc.
Voluntary Metric Framework Document (Recurring Document)
Purpose of requested Metric?
Metric Application?
Aggregate data?
ISP's already Collecting?
How reported?
ISP Comparative Data Envisioned?
Etc.
Standards Body or Industry Group
Assigned to Appropriate Industry Advisory Group(s)
ATIS
CSRIC Working Group
M3AAWG
Etc.
Pilot Program
Case Study
Standards Body Provides Structure for Case Study or Pilot Program
Standards Body or Industry Group
Standards Body Returns Formal Position, with metric definition, to the Metrics Board of Review
Example Definition
Data Filed with Industry Group under NDA
Anomomized
Technology Agnostic
Metric Option
1)
2)
3)
4)

9.9 SMALL AND MEDIUM BUSINESS CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4 March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY & INTRODUCTION

Welcome to the FCC's Communications Security, Reliability, and Interoperability Council IV (CSRIC IV) Working Group 4 (WG 4), Small and Medium Business (SMB) Feeder Group Report. This document is written for small or medium businesses in any of the five communications industry segments: broadcast, cable, satellite, wireless, and wireline.

At the outset:

- We congratulate you for exploring this resource.
- We recognize that undertaking a comprehensive, updated, and company-wide approach to cybersecurity may be difficult, especially given your company's size, operations, and limited access to financial, staff, and technical resources.

SMB stands for small and medium business, but we are not providing a proscriptive definition of what an SMB is, rather, as you read later, we outline some ways to think of your size and capabilities in relation to other communications businesses.

To understand what is happening in cybersecurity today, all you need to do is look to the latest headlines. Cyber-attacks have intensified in frequency, sophistication, and severity. Corporations, networks, and individuals are under constant attack by cyber-threats from within the United States and abroad. Internet services and communications have been impeded by attackers, causing disruption and uncertainty for millions of users. Personal information and corporate data have been stolen. And it is not just the big companies who are being attacked—small and medium size companies may be seen as easier targets or stepping stones to attack larger networks.

The need to protect your networks and customers is critical from both an infrastructure and a business perspective. As SMBs, you should continually strive to embrace new methods and tools, and, even more importantly, maintain cybersecurity resilience as a key and active part of your operations and business plans. Just as careful budgeting, the right equipment, and an understanding of your customers are key to keeping your businesses relevant and useful, ensuring your ability to continue to operate in the face of cybersecurity threats has become an integral part of your organization.

Rather than providing yet another checklist of things that need to be done, cybersecurity protection and resilience is best approached using risk/benefit analysis. The central resource for this effort is the "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.0 (*NIST CSF*), which was released February 12, 2014.[111] This risk management approach is flexible and dynamic in order to successfully respond to your environment, risk tolerance, and unique needs. It helps you to identify, assess, and prioritize the greatest risks to your business needs and functions. The *NIST CSF* then helps you determine where and how best to apply resources to minimize, monitor, and control the probability and/or impact of cybersecurity events.

[111] *See* National Institute for Standards and Technology, *Framework for Improving Cybersecurity*, 79 FR 9167 (Feb. 18, 2014) [hereinafter *NIST CSF*], *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

It is important to keep in mind that you are already making many risk/benefit decisions in the day-to-day operations of your business; while some of these concepts may appear new and require time to study and embrace, cybersecurity preparedness is, at its foundation, another risk identification and benefit analysis procedure, just as you already use every day.

The NIST Framework provides five "functions" that all organizations, regardless of size, can use to evaluate their cybersecurity programs:

- Identify – Develop understanding within an organization or operation to manage cybersecurity risks to systems, assets, data, and capabilities
- Protect – Develop and implement appropriate safeguards to ensure the delivery of critical services
- Detect – Develop and implement the capability to identify the occurrence of a cybersecurity event
- Respond – Develop and implement methods to respond to cybersecurity events that have occurred
- Recover – Ensure the ability to restore normal operations and to learn from the events that have occurred

Within each function, the NIST Framework provides more granular guidance via 22 specific "categories" and 98 "subcategories."

The following report explains, in basic terms, how to interpret the NIST Cybersecurity Framework. It provides illustrative examples of how to apply the NIST Framework to protect your core network and critical infrastructure. The guidance provided within this report is designed for an SMB that is seeking to undertake a more formalized and structured risk-management approach to address cybersecurity. However, each company should evaluate and apply the NIST Framework based upon its unique needs and operational environment.

In closing, we invite you into the cybersecurity conversation. While the CSRIC IV committee has a specific finite life, your participation in improving our country's cybersecurity resilience is critical to protecting our nation and our customers.

II. FEEDER GROUP STRUCTURE

The SMB Feeder Group consists of representatives of small to medium businesses from each of the communication segments: broadcast, cable, satellite, wireless, and wireline. Those individuals are listed below.

Name	Company
Adrienne Abbott	**Nevada SECC**
Edward Czarnecki	**Monroe Electronics/Digital Alert System**
Seton Droppers	**PBS**
Chris Homer	**PBS**
Susan Joseph (Co-Chair)	**CableLabs**
Kevin Kastor	**Consolidated Communications**
Jeremy Larson	**SilverStar Communications**
Greg Lucak	**Windstream**
Joel Rademacher	**Iridium**
Bill Trelease	**Delhi Telephone Company**
Jesse Ward (Co-Chair)	**NTCA – The Rural Broadband Association**
Kathleen Whitbeck	**Nsight**
Pam Witmer	**Pennsylvania Public Utility Commission (PUC)**

III. BACKGROUND

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," (EO) in February 2013. It directed the National Institute of Standards and Technology (NIST) to lead the development of a technology-neutral, voluntary Cybersecurity Framework to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

NIST released the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.0 (NIST Framework) on February 12, 2014. The NIST Framework, created through collaboration between industry and government, consists of existing standards, guidelines, and practices, and can be used by a variety of industries and organizations to promote the protection of critical infrastructure.

In March of 2014, the FCC established CSRIC IV WG 4 to analyze the NIST Cybersecurity Framework with respect to the communications sector and address how communications companies can apply the NIST Framework within their organizations to strengthen and protect their networks and infrastructures against cyber threats and attacks.

Within WG 4, a Small and Medium Business (SMB) Feeder Group was created, containing representatives from all five communications segments: wireline, wireless, cable, satellite, and broadcast. The SMB Feeder Group focused on helping small and medium communications

companies understand how the NIST Cybersecurity Framework could be applied to their operations, while respecting challenges related to their size and limited resources.

IV. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objective

The SMB Feeder Group strived to advance awareness and education with regard to the importance of cybersecurity for small- and medium-sized organizations and worked to ensure that cybersecurity risk management "best practices" are flexible and scalable for companies of all sizes. As such, the SMB Feeder Group's objectives were as follows:

- Explain, in basic terms, why cybersecurity is important and what SMBs can achieve by using the WG 4 document to improve their cybersecurity risk management practices.
- Provide overall guidance on how SMBs can digest and apply the NIST Framework, while providing flexibility for individual companies to suit their unique needs, characteristics and risks (i.e., there is no one-size fits all approach to cybersecurity risk management.).
- Provide guidance with respect to prioritization of relevant NIST Framework subcategories from an SMB perspective.
- Develop at least one SMB use case.
- In coordination with the Barriers to Implementation Feeder Group, identify challenges that SMBs commonly face and explore ideas for mitigating them.
- Develop an annotated, refined list of resources/references/tools for SMBs.

B. Scope

Within CSRIC IV WG 4, the five industry segments were charged with adapting the NIST Framework to the communications sector based upon the need to protect the core network and "critical infrastructure" as defined by the EO112 and further outlined in the Department of Homeland Security's (DHS) 2012 National Sector Risk Assessment (NSRA).

Although many SMBs may not fall into the strict letter of the EO's definition of "critical infrastructure," they can adhere to the spirit of this assignment, thereby keeping the scope of the WG4 effort the same, but scaling it appropriately for SMBs within the communications sector. In other words, this feeder group's mission is to assist SMBs with protecting their "core network" and "critical infrastructure" as defined by each local operator or broadcaster.[113]

---

[112] *See* Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737, § 2 (Feb. 19, 2013) [hereinafter *EO 13636*] ("[As] used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.").

[113] The SMB group is not specifying or defining "critical infrastructure" and "critical services" for SMBs within the communications sector. Rather, this is an individual decision based upon an SMB's local area, its needs, and network capabilities. In addition, it is important to note that *EO 13636* defines "critical infrastructure" and then designates the determination of specific critical infrastructure operators to the Department of Homeland Security. Nothing in this report contradicts that structure.

For example, most network operators should maintain service to their core switch so that public safety answering points (PSAP), hospitals, and other critical customers can access communications services. In terms of a "small" or "medium"-sized local broadcaster, the organization should maintain and secure critical public services such as the emergency alert system (EAS).

Each of the industry segments has further defined the "core network" and "critical infrastructure and services" as it relates to large businesses, and this info may prove useful to SMBs as they also look to define those terms for their local areas:

- Broadcast – See Sections I and II of the Broadcast Segment Report
- Cable – See Section III of the Cable Segment Report
- Satellite – See Section II of the Satellite Segment Report
- Wireless – See Sections I and II of the Wireless Segment Report
- Wireline – See Sections I, II, and III of the Wireline Segment Report

Also of note, although the NIST Framework can and should be evaluated at the enterprise level, as this is a good business practice and corporate citizenship, this is not the spirit of the WG 4 effort. For SMBs in particular, it is most important for these resource-challenged organizations to start by protecting their core network, and critical infrastructure and services.

In addition, readers may question if their organization falls within the scope of this report with respect to the size of their operations. The Small Business Administration (SBA) has established a numerical definition of small businesses, or size standards, for all for-profit industries, which are helpful as a general guide.[114] However, whether a business is defined as "small" or "medium" for the purposes of this exercise is a complicated decision, based upon multiple intricate factors, and best left to the discretion of the individual business.

As it looks to self-classify with respect to size, an individual business should consider the following:

- the resources and/or assets that a "small" or "medium" business would have at its disposal to evaluate the recommended WG 4 best practices, including financial resources, the time required for the task, and a company's access to internal and external expertise;
- the role of a "small" or "medium" business in the supply chain, i.e. its purchasing power;
- the dependencies on outside consultants, partners, vendors, and systems, and the quantity/importance of those relationships;
- the total number of customers served by a "small" or "medium" business;
- the business drivers for security, i.e. the unique needs of the company's or organization's customers;

[114] Small Business Administration, *SBA Size Standards*, https://www.sba.gov/content/summary-size-standards-industry-sector (last visited Mar. 13, 2015).

- and, if a cyber-incident should occur within a "small" or "medium" business, its resultant impact upon a regional or local area.

C. Methodology

The SMB Feeder Group evaluated the 98 subcategories included within the NIST Framework. The group discussed whether each subcategory was in or out of scope; its criticality to protecting the core network and/or critical infrastructure from cyber threats; how it should or could be applied in a small or mid-sized carrier's or broadcaster's network; and potential barriers to implementation.

Based upon this analysis, from the 98 initial subcategories, the SMB group selected a subset of 37 high-priority subcategories. This culled list is a useful starting point for an SMB that is seeking to undertake a more formalized and structured risk-management approach to protect its core network and critical infrastructure and services from cyber threats. As determined and selected by the SMB group, the high-priority subcategory list, in its entirety, can be found in Appendix II.

Although the list may be a helpful starting point for those SMBs that are intimately familiar with the NIST Framework, others may need more substantive guidance with simplified language and recommendations. As such, based upon the high-priority subcategory listing, the feeder group created a narrative centered on three basic questions:

1. **What** does an SMB need to protect;
2. **Who** has the responsibility for a given task; and
3. **How** will an SMB protect its core network and critical infrastructure and services (i.e. develop plans for identification, prevention, recovery, and continual improvement)

The SMB Feeder Group also developed use cases based upon the high-priority subcategory listing contained in Appendix II. The entirety of the Results and Findings analysis discussed below – including the "What," "Who," and "How" narratives and the Use Cases – should be taken as a whole and provide SMBs with practical guidance with regard to how they can digest and apply the NIST Framework to protect their organizations' core networks and critical infrastructure and services.

It is important to reiterate that the guidance provided in this document is designed for illustrative purposes only, and should not be boiled down to a prescriptive, inclusive list that pre-defines which NIST Framework subcategories apply to all SMBs within the communications sector. Rather, consistent with the NIST Framework which provides for flexibility, each company should examine its network, core business objectives/mission, risk tolerance, and security needs to determine which subcategories—of the 98 included in the NIST Framework—are most applicable to its operations.

V. RESULTS AND FINDINGS

A. What

As mentioned previously, given its size and scale, an SMB may not be responsible for deploying and maintaining "critical infrastructure" as that term is defined in the EO. However, its ability to operate secure, reliable networks and provide protected, resilient services is no less important to the critical customers that may operate in its service territory such as public safety answering points (PSAPs), hospitals, law enforcement agencies, and educational institutions.

The ability of an SMB to protect its networks and services first depends on answering a seemingly simple question – what are you trying to protect? This is the critical component of the "Identify" function in the NIST Framework. Identifying all of the elements within a network that need protecting is the prerequisite for managing the remaining four functions in the NIST Framework – Protect, Detect, Respond and Recover.

The answer to "What" should encompass physical assets, devices and hardware, as well as software platforms and data applications. For instance, wireline and wireless providers likely will identify their home location registers (HLR), SS7 protocols, and voice switches as part of their core networks or critical infrastructure. For cable operators, network operations centers (NOCs) and core routing facilities likely would be self-classified as critical infrastructure. Satellite uplinks likely would be classified as critical to satellite providers, while broadcasters likely will classify satellite uplinks and location transmitter sites as critical components. However, it can be a challenge for SMBs to identify all of their assets, particularly if this type of record keeping is not part of the current business culture, or acquisitions have combined networks with varying degrees of available inventory details. An inventory method can be as simple as a regularly updated spreadsheet or as complex as a software platform integrated into network operations. (ID.AM-1 and ID.AM-2)

Once an effective inventory system is in place, all assets should be reviewed and prioritized to determine if they are part of the organization's core network and critical infrastructure and services. This prioritization will assist in identifying where potentially limited resources should be directed in order to maximize the ability to secure unprotected systems or eliminate unauthorized or unnecessary software. Identifying and addressing the most critical vulnerabilities first can lead to large steps in developing a cybersecurity risk management strategy. (ID.AM-5)

Be cautious not to operate with tunnel vision; for example, you likely recognize that if your core router were compromised it would have a serious impact to your network, but how about all the workstations that can access the network elements? Compromising a workstation may give a bad actor access to the router, even if the later has all its security patches installed. To set priorities, it may be useful to start from the inside and work out; identify core, critical infrastructure and business assets, as they will have the highest priority with respect to network protection techniques, i.e. the most frequently updated, monitored, tested and backed up, which will enable the fastest recovery if ever necessary. Facilities that have direct access to high-priority assets, such as workstations, element management systems and your network monitoring system that has access to all core

assets, likely will be the second priority and as we get further from core assets, the lower the priority.

With assets inventoried and prioritized, the network is now ready for a targeted, efficient monitoring program that can protect the most critical network elements from vulnerabilities within the system or threats generated external to the system. This can provide a baseline against which an SMB can better police and control the flow of traffic through their network. However, continual monitoring can be a sizeable step for an SMB, which is why prioritization is so vital. (ID.RA-1)

Another aspect of "What" includes the type of activity to be evaluated once a monitoring program has been established. Access to physical assets, both internal and remote, the presence of unauthorized code or malware in the network and personnel or third-party service provider activity are common targets for monitoring and, in many instances, may yield proportionally large benefits relative to the resources required. Investigating and acting on notifications from monitoring systems will prepare an SMB for the remaining four NIST Framework functions (Protect, Detect, Respond, and Recover) and enable it to better withstand a cybersecurity event. (DE.CM-1, DE.CM-2, DE.CM-4, and RS.AN-1)

B. Who

Cybersecurity cannot be properly implemented without understanding the individual roles and responsibilities as they apply across all of the NIST Framework categories (Identify, Protect, Detect, Respond, and Recover). Cybersecurity awareness is not just for IT or network engineering personnel but for all employees, contractors and vendors. Especially in an SMB where resources are limited, it will require all employees to be vigilant in doing their part to protect the core network.

First and foremost, cybersecurity needs to start with senior management and the importance needs to be communicated to all employees. In many organizations, this is part of the company's on-boarding process. In order to establish proper security configurations, the system administrator needs to understand individuals roles and responsibilities and identify who needs access and at what level. The system administrator can be an individual, a group of individuals, or a contractor who has responsibility for the network. Even more important, privileged users need to understand their roles and responsibilities. (ID.AM-6, PR.AT-2 and PR.AT-5)

Once roles and responsibilities are established, processes need to be put in place to ensure proper communications during an incident and for continuous improvement. Incident management can be as simple as an escalation phone tree that starts from the bottom of an organization and extends to those who need to know, from an on-call employee who recognizes an issue, to technology personnel, and eventually to company leaders. Or, a more formal service management process can be used, which includes specialized software for logging and tracking incidents. (RS.CO-1 and RS.CO-4)

It is recommended that governance be established to include both technical personnel and stakeholders from all departments to provide a platform for continuous improvement.

Each department within an organization needs to be involved including, but not limited to, Technology & IT, Operations, Finance, Sales and Human Resources. Third-party contractors and vendors supplying subject-matter expertise, in addition to pertinent information from government agencies and the web blogs should also be consulted. (ID.GV-4)

We recommend developing security-related policies that have the support of senior management, are taught and enforced throughout the organization, and are reviewed and updated frequently. A security-mindset needs to be ingrained in the organization as to approximate a life style. These plans will address basic security processes like locking doors and changing passwords, to more specific recommendations concerning network equipment configuration recommendations, logging and backups. Although memorializing a security policy on paper is a good starting point, even more important is a company-wide commitment to security through training, and living the policies through encouragement or enforcement.

C. How

In the previous two sections we discussed what you need to protect, and who is responsible for protecting it. The last critical piece to this picture is how you can protect your critical facilities from potential cyber threats or attacks.

This process begins with identifying potential cybersecurity risks and threats to your network, assessing their likelihood, evaluating how they will affect your network, and, finally, defining how you will respond to those risks. This analysis is articulated in a risk management plan. A risk management plan needs to be flexible because no one can predict the future with a high degree of accuracy; rather, plans have to address known possibilities and be adaptable for unknown events. Just as we anticipate and strive to prevent unintentional human error from degrading our networks, we can, and should, anticipate network congestion (i.e. the impacts of distributed denial-of-service attacks (DDoS)). Likewise, we should be able to predict and prevent unauthorized access, and we should be able to harden our networks from known vulnerabilities. (ID.GV-4)

Since predicting future threats may be difficult, we should look to secure our networks and develop plans to address known attacks. This also will ensure we have a variety of tools in place to help us deal with or at least mitigate new threats. Companies should look to available sources to determine threats and remediation techniques. Many equipment and operating system vendor websites provide information on known threats and the recommended patches that can be installed to protect against them. Anti-virus companies provide updates, removal applications, and/or processes to detect and prevent computer viruses on various systems. The United States Computer Emergency Readiness Team (US-CERT) "leads the effort to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks."[115] Companies can subscribe to the US-CERT mailing lists and news feeds to get up-to-date information on the latest

[115] *See* U.S. Computer Emergency Readiness Team, *About Us*, https://www.us-cert.gov/about-us (last visited Mar. 13, 2015).

system/software vulnerabilities and the associated patches. SMBs should assume that threats that vendors, security developers, and US-CERT know about and have addressed are extremely likely to affect their assets. (ID.RA-5 and ID.RA-6)

Now that you identified potential threats to your network, you need to work on ways to keep them out of your network. Access control mechanisms can be used to restrict and limit who and what has access to your network(s). Previously, in the "What" section, we suggested prioritizing assets from the "inside out." However, the "outside in" approach works well for implementing access control security measures. Using the "outside in" approach, a company implements security at the most general levels then works toward the details both physically and logically. SMBs should start by limiting access to physical facilities containing core network elements, critical infrastructure, and mission-critical equipment, and developing a mechanism to confirm that the person trying to gain access has a need, status-level, and/or permission to enter those facilities. (PR.AC-2, PR.PT-3 and PR.PT-4)

Logical access follows the same methodology. Place generic restrictions at the edge of the network, typically at a router, which connects to the public Internet. Use access control lists (ACLs) to filter clearly inappropriate traffic such as "private" IP ranges, or some IP range and protocol combinations. Establish a firewall to block everything that originates from outside a network with only specific exceptions enabled, such as VPNs (virtual private networks), which are configured and authenticated per person. (PR.AC-3)

Inside the SMB's network (behind the firewall relative to the public network(s)), access is further restricted by user groups and individual responsibility requirements. Application networks should be divided by customer support systems, accounting/billing, and network equipment/element management systems, and isolated with ACLs that limit which workstations or systems have visibility into each network. (PR.AC-5)

In order to ensure systems are configured correctly, it is advisable to test system configurations frequently. There are open source and commercial tools that perform these tests. *Use caution to target the correct devices.* Check the perimeter router to confirm the allowable destination and source IPs and ports respond as expected. Next, run the same tests against all workstations, servers, and network elements from other "internal" networks, and their own network. Internal scans should include the whole possible network range; it is a good way to confirm documentation of existing equipment (new or removed) as well as the configuration(s). (A component of ID.RA-5)

User access to systems (user credentials) and the actions they can perform (view, update, administration, etc.) are restricted by user requirements. User credentials should be centrally managed in order to ensure consistent security across all accounts. Where possible, network elements should authenticate against the central system; those that cannot, should have appropriate user levels configured correctly and use unique strong passwords for each account. ACLs should limit element access to only those that originate from corporate network workstations. Vendors or others requiring only occasional access

should have their credentials enabled only upon request and disabled immediately after task completion. (PR.AC-1, PR.AC-4, PR.PT-3 and PR.PT-4)

Once systems have been configured, any changes to those systems must be managed and approved to ensure the integrity of the network is maintained. Change management defines the processes and procedures that are performed when an asset or software application within an infrastructure needs to be modified or updated. The reason for the change and how it impacts dependent assets or software needs to be understood and accepted. (PR.IP-3)

All SMBs will require remote maintenance at one time or another. Vendor and consultant access should be limited, enabled as required, and disabled immediately following the work being completed, while "trusted" employees should probably have minimal restrictions on their connectivity with all "local" access restrictions applying to their remote connection. Firewall logging should be enabled. In addition, there are several reasons to discourage or prohibit remote control applications (like LogMeIn) in favor of client-based VPN. For instance, remote-control applications bypass firewall logging and centrally managed authentication. (PR.MA-2)

Risk management philosophy implies constant evaluation of current status and changes in the environment. When notifications of newly discovered vulnerabilities are received, SMBs should take appropriate action(s) including installing patch fixes and/or upgrades, replacing equipment, or documenting the vulnerability as an acceptable risk presumably due to its low potential impact on the network or the business. (RS.MI-3)

It is unlikely that an SMB within the communications industry will be able to completely avoid being the victim of a cybersecurity incident; however, the company can be prepared to minimize the scope and duration of the incident. Several of the preceding recommendations address aspects like isolating networks (limits the scope to the compromised network segment), unique passwords (limits the incident to a single device, although it may have wide reaching affects), and frequent backups and recovery testing (assists with limiting the duration of an event). Minimizing an incident in progress is challenging, and may require the cooperation of several players including SMB experts, equipment vendors, and service providers. One way to minimize an event in progress is to activate "spare" equipment, which has been previously configured, to replace a compromised unit. Lacking 100% spares, a company may have to face the possibility that turning down a service or network segment may be the most expedient means of response and recovery. (RS.MI-1 and RS.MI-2).

VI. USE CASES

In this section, we have provided two use cases that describe the steps taken by two SMBs when implementing the NIST Framework within their organizations to protect their core networks and critical infrastructure and services. The use cases describe both a high-level business methodology as well as a technical/engineering component.

There are many approaches that can be taken to use the NIST Framework; as no two companies are the same, their approach will be different. However, after undertaking the NIST Framework process, all companies should experience the same result: an increased resiliency and ability to maintain critical infrastructure and core networking functions in the face of cybersecurity threats and attacks.

A. Broadcast Industry Use Case

As a local radio and television broadcaster, I have a commitment to my community for which my station is licensed. Making cybersecurity an intrinsic part of our business protects our revenue, employees, viewers, and community at large.

Unfortunately, we were recently hit with a virus that infected the computers in our newsroom, and, within a half-hour from the time of detection, every machine in our station technical center, except for the master control system, had been infected. The virus was brought in from one of our field reporters' laptops. Based upon this experience, our station management decided to review and then use the NIST Framework to protect our core network and critical infrastructure.

The areas that we focused on were access points to our critical business and broadcast systems. This involved applying the principles of the NIST Framework to protect our inbound/outbound firewall, the broadcast DMZ that separates the broadcast LAN from the administration LAN, and laptops and "thumb" drives.

As the Chief Engineer, I compiled information from our local security consultant and from various government websites. My Station Manger then set up a meeting with all the department heads from Sales, Programming, Finance, News and Engineering and I presented on the NIST Framework and the guidance for small businesses from the information found while working on the WG 4 report. It was helpful to have a diverse group of stakeholders in the room as cybersecurity is everyone's responsibility, and it requires buy-in from all staff members.

As a group, we reviewed the 98 subcategories within the NIST Framework, and based upon our initial risk assessment, what had the greatest urgency to be implemented within our network. We then devised a plan for review and recommendations with respect to the following categories:

1. ID.AM-6 Asset Management – Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established.

2. ID.GV-4 Governance – Governance and risk management processes address cybersecurity risks.
3. ID.RA-3 Risk Assessment – Threats, both internal and external, are identified and documented.

Once we completed our analysis, we then moved to implementation. This was actually a bit easier once we understood "what" needed to be done, "who" was responsible and "how" to move forward. During this implementation we focused on the following;

- PR.AC-1 Access Control – Identities and credentials are managed for authorized devices and users.
- RS.RP-1 Data Security – Response plan is executed during or after an event.
- PR.IP-3 Configuration change control processes are in place.
- DE.CM-1 Anomalies & Events – The network is monitored to detect potential cybersecurity events.
- RS.CO-1 Communication – Personnel know their roles and order of operations when a response is needed.

As you can see, it is not only important to place cybersecurity controls within the network, but to change the "culture" so that people are aware of cybersecurity risks and their related responsibilities. We are fortunate that our station has the necessary components available. For instance, a firewall was already in place, but we simply did not go far enough in protecting ourselves from cyber risks.

We were lucky as we were hit with a simple virus and the clean up only took a day. That was enough to start taking cybersecurity seriously. Since that "day" we now have employees trained in their role in cybersecurity, protection on all devices including laptops and thumb drives, and continuous monitoring and improved security within our routers and firewalls. We now track all system changes and incidents through our new service management system.

We also now have regular meetings with our new "cybersecurity committee" to discuss the latest threats, changes to our security protocols, and next steps for implementing the NIST Framework. Each quarter we review the NIST Framework against our business and look for new ways to improve our systems and processes.

B. Wireline, Wireless, and Cable Use Case

As a small or regional communications provider, we do not have a national scale, but we have equally important regional and local communications needs as we are, in some instances, the only carrier serving critical anchor institutions within the community. A targeted cybersecurity attack could reduce response times, eliminate communication, or provide misleading information during a disaster.

This use case focuses on the public-facing network that affects the communication for our customers. A business or company should take responsibility for ensuring that its core

network and critical infrastructure and services adhere to industry best practices and regulatory requirements. The high-priority items identified in Appendix II should be applied to harden against external and internal cyber-attacks.

- *ID.AM-1: Physical devices and systems within the organization are inventoried*
- *ID.AM-2: Software platforms and applications within the organization are inventoried*
    - All companies, regardless of size, should maintain a list of equipment required for critical services. This list can be as simple as an Excel spreadsheet or as complex as an automatic system documenting the network. We recommend tools that can gather this information and produce some type of report(s). An inventory system can be used to verify that software patches that have been identified by the manufacturer or third-parties have been applied. **You can't protect what you don't know.**
- *ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value*
    - The complete inventory list should be prioritized by value inside your communications infrastructure. Items critical to all of your customers or critical to emergency responders should be given priority for upgrades and patches. These critical items could be the most vulnerable because they are Internet terminations devices, core router(s), or long-haul transport systems.
- *ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established*
    - Knowing the cybersecurity roles and responsibilities can be an overwhelming task. In most companies, all personnel do not have access to the company check book or accounting software. Cybersecurity is no different; you need to define who is responsible for protecting the network. You need to establish a clear chain of command in the event of an attack to guide the process of recovery and reporting.
    - Outside contractors and vendors are a lot harder to get a handle on for a small provider, and even worse for a medium provider. We recommend you start by sending out an internal survey to find out who has access to your networks; this could include network support for equipment, accounting auditors, regulatory consultants, and even HVAC contractors. Once the list is established, create your requirements or questions, and have each vendor complete the form. We recommend denying access to the networks until the forms are completed.
- *ID.GV-4: Governance and risk management processes address cybersecurity risks*
    Processes do not create a secure network, but they provide guidelines to make sure a company is complying with regulations. Cybersecurity needs to be part of your company's risk management process. No network is completely secure and different levels of security require different financial requirements. Risk versus security needs to be included in the risk management process. This risk management can be an informal process, or a risk report to show and measure progress.
- *ID.RA-1: Asset vulnerabilities are identified and documented*

  - In the Identify section we identified our network and the equipment inside our network. We should now review the items and identify the known risks to the devices. You need to understand which devices have the highest cybersecurity risk based on their importance in your network plus their vulnerabilities. If your devices must run simple network time protocol (SNTP) for monitoring, then these devices should be listed as being vulnerable to an SNTP protocol attack; likewise, if these devices must respond to network time protocol (NTP) messages, they are vulnerable to an NTP type attack. Devices running multiple services and protocols will be more vulnerable to attacks.
- *ID.RA-3: Threats, both internal and external, are identified and documented*
- *ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk*
  - Documenting threats is important for all businesses, regardless of size. A group or individual exercise to identify threats to the organization will help an SMB focus on this effort while utilizing its limited resources. An example would be having the managers/technical staff identify the top five internal and external cybersecurity threats. These could be compiled into a complete list to allocate capital and personal resources.
- *ID.RA-6: Risk responses are identified and prioritized*
  - Identifying risks is the first step in mitigating the risks; the identified and prioritized list should be used to create plans for mitigating the identified problems. Cybersecurity is a continual process; companies should review the list of priorities on a scheduled basis.
- *PR.AC-1: Identities and credentials are managed for authorized devices and users*
  - Unauthorized access to devices is a critical vulnerability. All devices should be configured to use a username/password for access, or at least a complex password. When new equipment arrives from a manufacturer, it is configured with a default password. The default password needs to be reset to block unauthorized access to the device. Only authorized personal should know the password and it should not be stored in an unencrypted area to prevent a compromised computer from allowing a hacker access to the network. We recommend installing a centralized authentication system, which allows for an authentication policy to be implemented on one device and provides the ability to monitor access, logging it as it occurs.
- *PR.AC-2:Physical access to assets is managed and protected*
  - The best way to access any equipment is to be physically connected to the equipment. Physical access should be managed to prevent unauthorized access. This could be as complicated as a physical card reader system with surveillance cameras at each location, or as simple as making sure the database center/central office door is locked. In our use case, we installed a system-wide proxy card system and surveillance cameras to control and monitor access from a central location. As a small business, we felt that the centralized control and monitoring approach was our best use of capital to secure our network.
- *PR.AC-3:Remote access is managed*
  - Remote access is very important to companies that operate 24/7. Employees need to have access to equipment and data to perform their job while away

from the office. Remote access should be implemented with a two-step authentication process (one password to access their laptop and one password to access the network). With a one-step authentication process, if a laptop is compromised, then the attacker will also gain access to the network. In a two-step system, the hacker may have access to the computer, but will not have the password to access the network. We implemented a system of dual passwords, one to access network computers and one to get access to the network remotely.

- *PR.AC-4:Access permissions are managed, incorporating the principles of least privilege and separation of duties*
- *PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality*
    - Permissions need to be correlated within the company policy. These permissions should be extended to all devices in the network. The simple and very unsecure approach is to allow everyone access to everything, but this will create a very unprotected and unsecure network. All devices should be configured with some form of access control based on the user; this could be simply no access for users that do not require access, a read-only capability, privileged accounts which allow limited/authorized access, and finally an admin person who would have full access.
- *PR.AT-2: Privileged users understand roles &responsibilities*
- *PR.AT-5: Physical and information security personnel understand roles and responsibility*
    - We recommend all SMBs provide formal/informal training to new and existing employees about the critical assets under their control. They need to understand their role in providing and protecting critical services.
- *PR.AC-5:Network integrity is protected, incorporating network segregation where appropriate*
- *PR.PT-4: Communications and control networks are protected*
    - All SMBs should be deploying network segregation at some level. We expect all companies to separate the public and private networks. We also recommend that private networks be separated by roles for integrity. One large LAN for computers and equipment management puts both the equipment and LAN computers at risk. If the networks are separated, controls based on company policy can be applied to limit access to the network. Limited access reduces risk because it reduces the type of traffic and the source of the traffic to the equipment.
- *PR.DS-1: Data-at-rest is protected*
    - Data-at-rest is protected could mean a variety of levels of protection. For an SMB, simple procedures should be followed to protect data, including not leaving data outside the isolated network.
- *PR.DS-2: Data-in-transit is protected*
    - Data-in-transit should be protected when it leaves isolated and protected networks regardless of network size or business size. Data in transit which is not protected could be viewed and used for a cybersecurity attack. We recommend

encrypted VPN connections, encrypted virtual desktop connections, SSH, and SFTP for remote access. Use of any standard FTP and Telnet should be limited because they do not protect data in transit.

- *PR.IP-3: Configuration change control processes are in place*
  - We recognize that processes place additional work and burdens on SMBs who do not have dedicated staff to manage processes and cybersecurity. However, we recommend all communications providers implement a formal or informal process for configuration control. All proposed changes should be examined to make sure they do not violate company policy or standard cybersecurity practices. This could be a formal process or an informal process; it is partially a culture change to make sure cybersecurity is front-and-center during the network configuration process.
- *PR.IP-4: Backups of information are conducted, maintained, and tested periodically*
  - All companies should maintain backups of the network. A network can never be protected from all cybersecurity risks. Backups allow a network to be fully restored to an original configuration. Having backups available helps to reduce network restoration time. Network backups should be performed after significant changes and/or on a schedule. Multiple free or commercial software packages are available for configuration or system backup.
- *PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed*
  - A response plan can be a simple flow chart that provides a list of contacts that need to be contacted during an attack or recovery. We recommend, at a minimum, to create a flow chart showing who to contact for what type of attacks. For instance, you do not need to contact the CFO for a DNS/NTP attack, but a CFO should be notified of an attack against company financial data.
- *PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access*
  - If keeping someone physically away from the equipment is important, then making sure they don't have remote access is just as important. In some areas, remote access is even more important because the threats will come from outside the area. Remote access to equipment should be controlled; the best solution is to keep all management systems behind a firewall or control access by IP address. In our case, we built a separate network using VLANs and L3VPNs to separate monitor/control networks for our equipment. This control network is only accessed from our internal network or through a two-level authenticated firewall (key + username/password). The outside equipment has access lists applied to only allow IP address from our internet network
- *DE.CM-1: The network is monitored to detect potential cybersecurity events*
- *DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events*
  - The size of your business should not stop you from monitoring your network. Free tools like MRTG/Cati or Nagios should be deployed to monitor and baseline the network. Cybersecurity attacks can come in multiple forms and some can

cause huge network spikes. Using monitoring tools on the network allows these attacks to be identified and corrected.

- *DE.CM-2: The physical environment is monitored to detect potential cybersecurity events*
    - Cybersecurity incidents can originate remotely or through local attacks, and, as such, the physical equipment should be monitored to detect local attacks.
- *DE.CM-4: Malicious code is detected*
- *DE.CM-5: Unauthorized mobile code is detected*
    - Malware detection and antivirus software should be installed and maintained on all computers. Malicious code is a way to gain access to a network to cause problems. This detection software could be located on each device, plus on the ingress/egress network point to watch for anomalies in the network.
- *RS.RP-1: Response plan is executed during or after an event*
    - Businesses (small or large) need to have a response plan to describe what a company should do during an event. This plan could be an informal plan (something agreed upon verbally) but it is better if the plan is more formal and explains how to handle a cybersecurity event. In our plan, this included: who needs to be contacted internally (C-Level, Legal, and Network Manager); who is authorized to speed up mitigation, shut down all remote access, disable all internet traffic, disable a BGP session, and install an access list. By providing direct authorized items you can increase the recovery/mitigation timeframe.
- *RS.CO-1: Personnel know their roles and order of operations when a response is needed*
- *RS.CO-2: Events are reported consistent with established criteria*
- *RS.CO-4: Coordination with stakeholders occurs consistent with response plans*
    - Most likely, SMBs will not have staff dedicated to cybersecurity risk management. These roles will be filled by multiple personnel and completed as part-time work. Part-time roles enforce the need for response plans and reporting systems. If you employ full-time security personal, they understand the flow to resolve a problem. In an SMB, part-time roles require information and procedures to ensure polices are followed. By themselves, policy and procedures never make a network secure, but they allow conformity to make sure all parties are informed and information is documented.
- *RS.AN-1: Notifications from detection systems are investigated*
    - We understand that detection systems will not be part of all network plans due to their cost and complexity. If detection systems are used within a network, these systems should be configured for remote alerting or active monitoring in order to ensure an immediate response to cybersecurity attacks. We recommend, at a minimum, setting up system logging on all devices and using free off-the-shelf commercial software platforms to record data. Logging of the data will not be as robust as a dedicated detection system, but will provide data that can be used for root cause analysis.
- *RS.MI-1: Incidents are contained*
    - Cybersecurity incidents should be contained within a network. This may include shutting down the effected equipment, shutting down a user, or removing

access to the device completely (both ingress and egress). This process should be automated in a large company, but requires a manual intervention in an SMB.

- *RS.MI-2: Incidents are mitigated*
  - Once an incident has been contained, the second step will be to find the root cause and then correct the issue. If the original problem is not corrected, the attack or incident could happen again.
- *RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks*

SMBs must review any identified vulnerabilities through government and industry sources. We recommend each identified vulnerability be researched to find out the risks. We understand the limited resources of an SMB, but major vulnerabilities must be compared to risk.

VII. CONCLUSIONS AND RECOMMENDATIONS

- SMBs should avoid a checklist approach to cybersecurity. Cybersecurity is constantly evolving as technology advances, attack parameters change, and new threats emerge. A static checklist methodology is no longer an effective defense, as it confines the methods and tactics by which an organization can prepare for or respond to eminent threats. Rather, a more fluid and dynamic risk-management approach is needed. SMBs in the communications sector should revise their cybersecurity practices with respect to a risk management maturity model, consistent with the NIST Framework and the guidance provided in this document.

- SMBs should approach cybersecurity risk management as a process and strive for continual improvement. SMBs should ensure that they re-evaluate their security needs, current status, target state, and subsequent tasks on a re-occurring basis, with an eye toward process integration.

- Continued outreach is needed to ensure that the SMB community is engaged in the network risk management discussion generally, and aware of the benefits of the NIST Framework specifically. As NIST, DHS, and the FCC continue their outreach, they should understand that a single method of outreach may not be successful in conveying relevance to an SMB. To truly reach the SMB community, outreach should be structured in more practical terms, similar to those discussed in this document that talked about “What,” “Who,” and “How.” Likewise, SMBs should avail themselves of the resources and references that are available to them, including through the FCC, DHS, and the tools outlined in Appendix III to this report.

- Consistent with the approach taken in this WG 4, the FCC should continue to allow industry to evolve the CSRIC cybersecurity recommendations with respect to SMBs. The SMB Feeder Group has developed practical, actionable guidance for SMBs, and, in the future, industry is best positioned to revise and evolve the guidance issued in this document.

VIII. APPENDICES

The SMB Group includes the following appendices to provide resource-challenged SMBs with additional guidance in regard to cybersecurity risk management.

A. Appendix I: Barriers to Implementation

The Barriers to Implementation Feeder Group developed a detailed analysis of the various challenges faced by communications organizations as they attempt to apply the NIST Framework to protect their core networks and critical infrastructure and services from cyber-attack, including Financial, Legal, Technology, Consumer/Market, and Operational challenges.

The Barriers to Implementation Feeder Group explored each of these barriers, including which type of barrier presents the greatest obstacle to specific Framework categories and subcategories. For detailed information in regard to these five overarching areas of barriers, readers should consult the Barriers to Implementation Feeder Group Report. However, it is worth reiterating that as organizations defend their infrastructure from attacks by capable adversaries – especially small, resource-challenged organizations – they face significant challenges, including access to financial capital, operational manpower, technical expertise, management buy-in, and the tools and resources needed to effectively and efficiently create, maintain, and evolve a cybersecurity risk management program, among other barriers.

To overcome these challenges, SMBs should consider:

- Accessing the practical guidance within this report, and programs at DHS designed to assist small critical infrastructure organizations with developing or evolving a cybersecurity risk management program
- Pooling resources with their peers to gain economies of scope and scale
- Relying upon the support of their peers in the communications sector, chiefly communications operators and broadcasters, who have experience using the NIST Framework within their operations
- Availing themselves of “targeted incentives” that the government may provide in the future to satisfy the requirements of the EO

B. Appendix II: Priority Practices

As noted in the Methodology section above, the SMB Feeder Group examined the 98 subcategories contained within the NIST Framework. The group discussed whether the control was in or out of scope; its criticality to protecting the core network and/or critical infrastructure from cyber threats; how the given subcategories should or could be applied in a small or mid-sized carrier’s or broadcaster’s network; and potential barriers to implementation.

Based upon this analysis, the feeder group selected the subcategories that are the highest priority for an SMB that is just beginning to undertake a risk management process to protect its core network and critical infrastructure and services.

The following 37 practices were deemed to be the priority practices for SMBs to consider implementing as they provide a baseline of protection for critical infrastructure. However, it is important to remember that this is designed as merely a guide, and not a prescriptive, inclusive list that pre-defines which subcategories apply to all SMBs within the communications sector. Rather, each company should examine its network, core business objectives/mission, risk tolerance, and security needs to determine which subcategories—of the 98 included in the NIST Framework—are most applicable to its operations.

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
ID.RA-1: Asset vulnerabilities are identified and documented	What
ID.RA-3: Threats, both internal and external, are identified and documented	What
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	How
ID.RA-6: Risk responses are identified and prioritized	How
PR.AC-1: Identities and credentials are managed for authorized devices and users	How
PR.AC-2: Physical access to assets is managed and protected	How
PR.AC-3: Remote access is managed	How
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	How
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	How
PR.AT-2: Privileged users understand roles & responsibilities	Who

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
DE.CM-1: The network is monitored to detect potential cybersecurity events	What
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	What
DE.CM-4: Malicious code is detected	What
DE.CM-5: Unauthorized mobile code is detected	What
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	What
RS.RP-1: Response plan is executed during or after an event	Who
RS.CO-1: Personnel know their roles and order of operations when a response is needed	Who
RS.CO-2: Events are reported consistent with established criteria	Who
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Who
RS.AN-1: Notifications from detection systems are investigated	What

PR.AT-5: Physical and information security personnel understand roles and responsibility	Who
PR.DS-1: Data-at-rest is protected	What
PR.DS-2: Data-in-transit is protected	What
PR.IP-3: Configuration change control processes are in place	How

RS.MI-1: Incidents are contained	How
RS.MI-2: Incidents are mitigated	How
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	How

C. Appendix III: Annotated List of References/Resources

Included below is a list of tools, templates, reports, websites, etc., that can assist SMBs with their cybersecurity efforts.

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 OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Network Protection Tool	RAPID7	Penetration Testing Software	http://www.metasploit.com/	World's most used penetration testing software; Put your network's defenses to the test - A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments
Network Protection Tool	Sourcefire	SNORT	https://www.snort.org/	Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS).
Planning Guide	NIST	Contingency Planning Guide for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf	Provides instructions, recommendations, and considerations for creating a contingency plan that is used government agencies but can be applied to any company/industry.
Planning Guide	NIST	Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf	This document assists organizations in establishing computer security incident response capabilities and handling incidents.
Resource List	DHS	Stop.Think.Connect. Tips and Resources	http://www.dhs.gov/stopthinkconnect-get-informed	Materials that can be used to increase cybersecurity awareness.
Resource List	Maryland.gov	Department of Information Technology	http://doit.maryland.gov/cybersecurity/Pages/default.aspx	Provides link to cybersecurity resources and Maryland cybersecurity education sites.
Resource List	Multi-State Information Sharing & Analysis Center (MS-ISAC)	MS-ISAC Cyber Security Toolkit	http://msisac.cisecurity.org/resources/toolkit/oct14/	Near the bottom of this page are some documents created by the MS-ISAC to raise cybersecurity awareness through informative and practical means. There are also other cybersecurity resources and links on this page.
Resource List	United States Computer Emergency Readiness Team (US-CERT)	Getting Started for Business	https://www.us-cert.gov/ccubedvp/getting-started-business	Resources provided by the DHS Critical Infrastructure Cyber Community (C^3) to help businesses align themselves to the five Cybersecurity Framework Function Areas.

Resource List	US-CERT		https://www.us-cert.gov/security-publications/	Various publications to help a user from setting up a computer to emerging threats.
Self Service Tool	FCC	FCC Cyber Security Planning Guide	http://transition.fcc.gov/cyber/cyberplanner.pdf	A tool for small businesses to create customized cyber security planning guides.
Self Service Tool	FCC	FCC Small Biz Cyber Planner 2.0	http://www.fcc.gov/cyberplanner	Online resource to help small businesses create customized cybersecurity plans.
Self Service Tool	SBA	Cybersecurity for Small Businesses	http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses	This self-paced training exercise provides an introduction to securing information in a small business.
Self Service Tool	United States Computer Emergency Readiness Team (US-CERT)	Cyber Resilience Review (CRR)	https://www.us-cert.gov/ccubedvp/self-service-crr	The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. This site also provides a link to self-assessment tool.
Standards	Payment Card Industry (PCI) Security Standards Council	PCI Security Standards	https://www.pcisecuritystandards.org/security_standards/getting_started.php	PCI security for merchants and payment card processors is the vital result of applying the information security best practices in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data.
Training	FEMA	Cyberterrorism Defense Initiative	http://cyberterrorismcenter.org/	The Cyberterrorism Defense Initiative (CDI) is a national counter-cyberterrorism training program, developed for technical personnel and managers who monitor and protect our nation's critical cyber infrastructures. Classes are held in easily accessible and centralized locations throughout the United States.
Training	Infragard	The Center for Information Security Awareness	https://infragardawareness.com/	Infragard provides free online security awareness and PCI employee training for individuals. If you need a class they are willing to come out and brand the class for your company for a cost.

Training	MS-ISAC	Cyber Security Awareness Free Training and Webcasts	http://msisac.cisecurity.org/resources/videos/free-training.cfm	A collection of cybersecurity training websites and podcasts links.
Training	SANS	Webcasts	https://www.sans.org/webcasts/	SANS Information Security Webcasts are live web broadcasts combining knowledgeable speakers with presentation slides. SANS offers several types of webcasts designed to provide valuable information and enhance your security education.
Training	Texas A&M Engineering	Web-based Training	http://teex.com/teex.cfm?pageid=NERRTCprog&area=NERRTC&templateid=2039	The TEEX/NERRTC Cybersecurity web-based courses are designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure. These DHS/FEMA-certified courses are offered through three discipline-specific tracks targeting general, non-technical computer users, technical IT professionals, and business managers and professionals.
Training	US-CERT	CERT Podcast Series	http://cert.org/podcasts/index.cfm	A series of podcasts that provides both general principles and specific starting points for business leaders who want to launch an enterprise-wide security effort or make sure their existing security program is as good as it can be.

9.10 TOP CYBER THREATS AND VECTORS
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

TABLE of CONTENTS

I. EXECUTIVE SUMMARY

The growing popularity of mobile devices, applications, social networks, and Internet connected devices that make up the Internet of Things (IoT) makes the threat landscape a complex set of moving pieces. Today's cyber-attacks can appear to be simple and direct. But, they can also be deceptive in an attempt to distract from the primary attack objective. The entire threat ecosystem is made up of a diverse set of actors that are as intelligent, creative, deceptive, and often times more technically savvy than the networks, information, and the people that we are trying to protect.

Cyber attacker's motivations and their techniques continue to grow in number, complexity, and sophistication. The attacker's technical resources are constantly being developed, enhanced and reused throughout the entire threat lifecycle. Threat actors will continue to look for new vulnerabilities and attack vectors within every layer of the TCP/IP[116] and OSI[117] communications stacks.

While looking at the people, processes, and technologies required in identifying, protecting, detecting, responding, and recovering from cyber threats, as spelled out in the NIST Cybersecurity Framework (NIST CSF), the Threats Feeder Group has reviewed a set of processes for entities to manage their threat intelligence and then translate that knowledge into the most effective defensive actions. Tailored threat intelligence is powerful knowledge that allows entities to learn from the experiences of others, learn from their networks, learn from government, and industry subject matter expertise to potentially prevent malicious activity that might be otherwise difficult to identify.

There is a great deal of threat intelligence available from numerous sources; to be most effective however, the individual network operator seeking to protect its core infrastructure, needs to find the means to find the information relevant, or tailored, to that task. In particular, the Threat Feeder Group believes the Community Models for Threat Intelligence/Information Sharing and Analysis as outlined within the body of this report and manifested in sector-level ISACs should be considered by individual network operators.

II. INTRODUCTION

In support of CSRIC Work Group 4, the Threats Feeder Group was tasked to review the nature and trends of cybersecurity threats and with investigating ongoing processes that could be used to gather, analyze, categorize, and share information about threats and vulnerabilities relevant to the telecommunications sector. Threats and vulnerability information should be processed in a manner that can be rapidly and consistently identified and translated into defensive action by individual enterprises, segments, and the sector as a whole, in a manner consistent with risk-based decision making processes of an individual enterprise as well as the NIST Cybersecurity Framework. The work product of the Threats Feeder Group may provide

[116] *See* Wikipedia, *Internet Protocol Suite*, http://en.wikipedia.org/wiki/Internet_protocol_suite (last visited Mar. 13, 2015).
[117] *See* Wikipedia, *OSI Model*, http://en.wikipedia.org/wiki/OSI_model (last visited Mar. 13, 2015).

value to Communications Sector member companies in all five segments and across large, medium, and small size enterprises.

III. FEEDER GROUP STRUCTURE

The threats feeder group consists of the members listed below:

Name	Company
Co-Chair - Joe Viens	Time Warner Cable Inc.
Co-Chair - Russell Eubanks	Cox Communications
Chris Jeppson	Consolidated Communications
Tony Sager (Advisor)	Council on CyberSecurity
Brian Scarpelli	Telecommunications Industry Association
Kathryn Condello (Advisor)	Centurylink
Tom Soroka	USTelecom Association

Table 3 - List of Working Group Members

IV. BACKGROUND

Objective

The objective of the threats feeder group is to review current threats and trends and to investigate operational processes that could be used to better incorporate (gather, analyze, categorize) cyber threat, vulnerability, and intelligence information relevant to the communications sector, into risk management processes. Thus, the focus of this threats feeder group's effort is to best enable "threat informed" cyber risk management decisions.

The threats feeder group intends for the findings and recommendations in this report assist communications sector members of any size in participating in, and leveraging the information gleaned from community threat venues, to actively adapt to a changing cybersecurity landscape, and respond to evolving and sophisticated threats in a timely manner. Such approaches are the foundations upon which sector-level Information Sharing and Analysis Centers were developed as well as other organizations with varying degrees of formality. These venues are described in a recent draft NIST Guide to Cyber Threat Information Sharing[118] and are consistent with objectives described in a recently released Executive Order on Information Sharing.[119]

Scope:

The focus of the threats feeder group is on core communications networks. However the processes and models described herein could also be used to secure internal, enterprise networks as well.

[118] National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing (Draft)* 17 (2014), http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf.
[119] Exec. Order No. 13,691, *Promoting Private Sector Cybersecurity Information Sharing*, 80 FR 9347 (Feb. 13, 2015) (*EO 13691*).

The 2012 National Sector Risk Assessment Report was utilized as a core resource for this activity. The 2012 National Sector Risk Assessment Report for Communications was developed in a joint CSCC/GCC partnership effort in conjunction with our SSA, the Department of Homeland Security and other US Department and Agency representatives within the Government Coordinating Council.[120] The Assessment outlines ways that a bad actor could potentially take advantage of, or attack core communication networks. The Assessment further provided insights into the possible consequence associated with a cyber-attack on the core communications.

The threats feeder group agreed upon the following definitions of "threats". Threats are defined as intentional and unintentional attacks by both malicious and non-malicious actors committing resource exhaustion (affects network availability), system alteration (affects network integrity), and system intrusion (affects network confidentiality). [121]

The threats feeder group also chose to use the TCP/IP layered communications model, used by the CSRIC WG4 Ecosystem Feeder group as the reference model for analyzing threats.

The TCP/IP Model separates networking functions into discrete layers. Each layer performs a specific function and is transparent to the layer above it and the layer below it. From lowest to highest, the layers are the link layer, containing communication technologies for a single network segment (link); the internet layer, connecting hosts across independent networks, thus establishing internetworking; the transport layer handling host-to-host communication; and the application layer, which provides process-to-process application data exchange. In the context of this particular report, the Transport, Internet and Network Access (Link) layers, are the ones that are most likely to be implicated in the "core" infrastructure of concern to this working group.

[120] *See* Department of Homeland Security, *2012 Risk Assessment Report for Communications* 80 (Sept. 2012) [CLASSIFIED].
[121] *Id*. at 80.

TCP/IP Layered Communications Model

Hacker / Hacktivist / Attacker / Nation States / Criminal orgs / Exploit - Community

Enterprise / Government End Users

Network Operators /Network Providers / Communications Sector

Ecosystem category	TCP/IP Layers & Protocols	Cyber Attack / Threats
• Content producers/distributors • App developers/distributors • Operating Systems • Databases • Websites • Cloud (SaaS, PaaS+D36) Operator • OTT Operators • Network HW/SW/OS/CPE Vendors • Web Browsers • eCommerce Cos. • Edge Device Cos. • End User/Consumer • Relay Service Providers • Anti-Virus/Security HW-Firewall Vndrs • Public Safety Networks • Dark Exploit Websites • Open Source Community • Electronic Payment Networks	**APPLICATION** *HTTP, SMTP, SIP, INAP* *BGP, DHCP, DHCPv6, DNS, FTP, ONC/RPC,* *HTTP, IMAP, IRC, LDAP, NTP, POP,* *RTP, RTSP, RIP, SNMP, SOCKS,* *SSH, Telnet, TLS/SSL, XMPP*	• SQL/LDAP Injection • Email malware/Phishing attacks • HeartBleed/SSL Attacks • BrutPOS-Botnet against POS terminals • RAM Scraping malware • Cross-Site Scripting (XSS) • Cross-Site Request Forgery (CSRF) • Application Layer DDoS (e.g., malformed packet) • Masquerade Attacks & Exploits • Fraud/Theft/Customer record breaches • Distributed -Distraction DDoS Attacks • DNS Spoofing • CallerID Spoofing • Authentication/Certificate spoofing • Zero-Day/Watering hole attacks • Password theft & Keylogger Attacks • POS Intrusions/Trojans • DEV kit & SDK Exploits • Bitcoin Theft & spoofing • Rootkit Injection & Operations • USB 'Thumb-drive' injections & exploits • Zeus/Citadel "Man-in-browser" attacks • DNS Reflection Attacks
• Backbone Network Operators • Access Network Operators • Wireless Network Operators • Internet Service Providers • CDN Operators • Business VPN/VoIP Operators • OTT Operators • Utilities (private utility networks) • Cloud (NaaS) Operator • Internet Service Provider • Network HW/SW/OS/CPE Vendors • Edge Device Cos. • Social Media Cos. • Relay Service Providers • Anti-Virus/Security HW-Firewall Vndrs • Public Safety Networks • Electronic Payment Networks	**TRANSPORT** *TCP, UDP, RUDP, DCCP,* *CTP, RSVP, TLS, WAP, WTLS*	• Fraud/Theft/Customer record breaches • Man-in-the-Middle (MITM) • DDoS (e.g., traffic flooding, SYN flooding) • Eavesdropping • Network Reconnaissance • Session Hijacking/Session Poisoning • UDP Floods
• Backbone Network Operators • Wireless Network Operators • Utilities (private utility networks) • Cloud (IaaS) Operator • Internet Service Provider • Business VPN/VoIP Operators • Network HW/SW/OS/CPE Vendors • Edge Device Cos. • Anti-Virus/Security HW-Firewall Vndrs • Public Safety Networks	**INTERNET** *IP (IPv4 & IPv6), ICMP,* *ICMPv6, ECN, IGMP, IPsec* *DNS, DNSSec, MPLS*	• DDoS Attacks (e.g., traffic flooding, amplification - Smurf)) • IP Address Spoofing • DNS Cache Poisoning • Malformed Packet Attacks (e.g., Teardrop, Ping of Death, etc.) • Fraud/Theft • ICMP Redirect & Flooding • DNS Spoofing & Reflection Attacks
• Backbone Network Operators • Access Network Operators • Wireless Network Operators • Utilities (private utility networks) • Network HW/SW/OS/CPE Vendors • Edge Device Cos. • Internet Service Infras/Clearinghouse • Anti-Virus/Security HW-Firewall Vndrs • Public Safety Networks	**NETWORK ACCESS/LINK** *ARP/InARP, NDP, OSPF, Tunnels (L2TP),* *PPP, MAC(Ethernet), xDSL,* *ISDN, FDDI, DOCSIS, 802.11n, LTE-VoLTE,* *SS7, CDMA, GSM, 2G, 3G*	• MAC Address Spoofing & Flooding • ARP Cache Poisoning/ARP Spoofing • CallerID Spoofing • WiFi Intercept exploits • DDoS Attacks • SS7 (point code) Address Spoofing

V. FINDINGS

The Threat Feeder Groups reviewed a large number of publications (see Acknowledgements section). The following reflect key findings by the Threat Feeder Group:

A. Critical Infrastructure Findings

Cyber thieves, industrial/political spies, and cyber-criminals often operate within a company's own trust boundaries. Outbound threats are not always the result of an intentional attack. They often occur when an employee unintentionally opens a "back door" by downloading a rogue application, opening an email attachment, or by clicking on a web link that could infect and possibly drop malware on the employee's computer or edge device.

The Most Common Types of Cyber Threats to Critical Infrastructure (in general) include, but are not limited to:

- ***Proprietary Espionage*** - Targeted Information: Intellectual property; proprietary information; geopolitical, competitive or classified intelligence; etc

- ***Insider Trading Theft*** - Targeted Information: Pending M&A deals or contracts; upcoming financial earnings; future IPO dates; etc

- ***Financial & Identify Theft*** - Targeted Information: Employee and customer personally-identifiable information; payment transactions; account numbers; financial credentials; etc.

- ***Technical Espionage*** - Targeted Information: Password or account credentials, source code, digital certificates; network and security configurations; cryptographic keys; authentication or access codes; etc.

- ***Reconnaissance and Surveillance***: - Targeted Information: System and workstation configurations; keystrokes; audio recordings; emails; screenshots; additional infection vectors; logs; cryptographic keys; etc.

The most common Attacker Target/Data Loss events in and critical infrastructure systems are:

- Account passwords and hashes, password filter installation, group policy modification
- Intellectual & sensitive property, regulated and classified data theft
- Confidential records, column-level encryption
- Corporate communications, business & defense related data, early warning of detection
- Infections from partner organizations and agencies

In the area of targeted attacks against critical infrastructure, attackers are increasingly targeting:

- Specific populations (users within a particular political boundary)
- Geographic regions (users within a particular geographic boundary)
- Groups (users with shared roles or linkages: business functions, shared social habits, user communities)
- A single individual (a user chosen for strategic value)

Advanced Persistent Threat (APTs). The primary method for infecting targeted organizations involve sending spear-phishing emails to numerous targets. These phishing emails contain malware or malicious links to malware that exploits vulnerabilities found in popular operating systems, office applications, and programs. Attackers have successfully compromised organizations across every sector, including government and defense agencies, commercial enterprises, financial institutions, and scientific research facilities.

B. Communication Sector Findings

VoIP and Voice security threats within the Communications Sector can be placed into three classes of threats:

- **Availability Threats**: Availability of voice service refers to voice and VoIP service being available for use when needed. Just as with data networks, VoIP services are susceptible to a denial of service attack. Voice and VoIP distributed denial of service attacks can come from anywhere on the Internet or via the PSTN-SS7 networks. Another variation of a VoIP DDoS attack occurs when a cancel message is spoofed so that as a victim is unable to build a connection with the other party. As soon as a connection is established, a spoofed GOODBYE or a cancel signal is sent.

- **VoIP Confidentiality Threats**: When voice or VoIP confidentiality is compromised, information can be accessed by individuals that are not authorized to receive it. This type of threat includes unauthorized access to IP addresses, network documentation, system and endpoint passwords, audio/video content, conversation history, and call detail records. Eavesdropping of unprotected VoIP conversations is easier because there are a large number of nodes between two users and any of these can be used to access the IP packets that form the conversation. A large number of free and paid tools are available that allow VoIP packets to be converted to audio files. These audio files can be saved and played back later at leisure. Many VoIP phones and devices have a number of undocumented ports and services. These can be easily found by competent attackers and used to eavesdrop on conversations. Many VoIP systems for billing, call management, and routing are delivered and installed with default passwords that are well known to the attacker community.

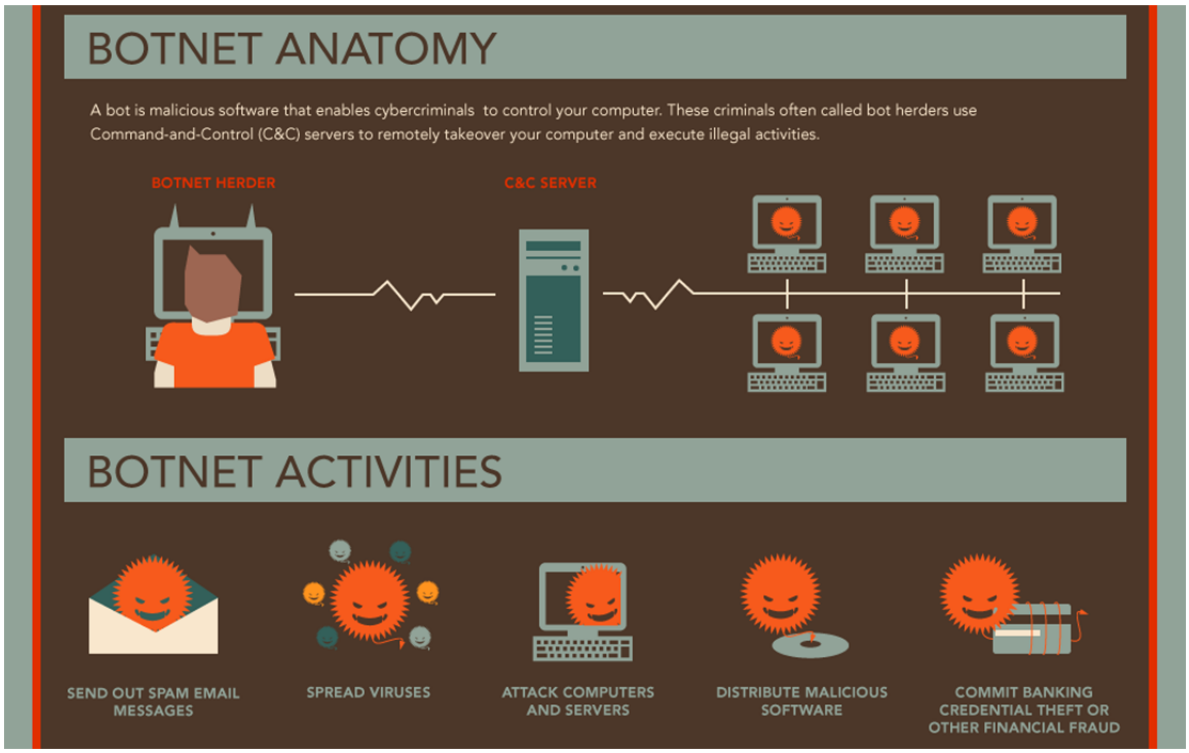
- **Voice & VoIP Integrity Threats**: Caller ID spoofing is one of the most prevalent voice integrity attacks and best known in the voice service provider community. Spoofed

caller IDs have been used to order cash transfers, Spammers also use Caller ID Spoofing techniques to launch attacks posing as banks or other trusted entities. Other integrity attacks rely on replacing a genuine client's information with that of the attacker. This will cause the call to be routed to the attacker. In a situation where the called party is not personally known, this could bring obvious benefits to the attacker – a scenario could be an attacker impersonating the help desk of a credit card company. Other integrity threats arise from techniques known as Registration Hijacking, Proxy Impersonation, and Call Redirection. In Registration Hacking, the attacker alters the registration details of the victim and inserts his (the attacker's) details instead. This will cause all calls for the victim to be routed to the attacker. A denial of service attack on the victim during this period ensures that the victim cannot attempt to re-register. During this period, the attacker can assume the VoIP identity of the victim. There is no simple method to prevent caller ID spoofing on which the entire series of Integrity Threats rest. Experts say that the best thing to do is not to trust caller ID display without other supporting evidence.

C. Bots and Botnets

The growing number of cyber attacks that indicate bots and bot nets as a go-to tactic for hackers and hacker groups. A bot is a computing system tasked with performing a specific Internet function in an automated fashion. Not all bots are malicious in nature; there are bots that perform legal and useful tasks such as Web indexing, data collection, competitive research, and promotional activities on social networking Web sites. For attackers, the benefits provided by bots include the ability for bots to perform maliciuos tasks repeatedly, quickly, and in an automated manner enabling attackers to control these systems en masse and to great effect. A group of coordinated bots, called a botnet, enable threat actors to perform distributed denial-of-service (DDoS) attacks on massive scales.

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



Source: Check Point Software Technologies

Key components of a large bot network includes, but not limited to:

- An address book of contacts or a collection of compromised servers (to act as watering holes).
- An email or web-based delivery mechanism.
- Socially engineered content for lure activation.
- Redirection servers and domains to mask destination.
- Hosted malicious content servers and domains for exploits and malware.
- Command-and-control (C&C) servers and domains for lateral movement within a targeted network, and further penetration.
- Data exfiltration repositories.

D. DDOS Attack

DDoS attack vectors within the Communications Sector can vary significantly. However, DDoS Attack vectors can fall into one of three categories:

1. **Volumetric Attacks**: These attacks attempt to consume the bandwidth either within the target network or service, or between the target network or service and the rest of the Internet. These attacks are simply about causing congestion.

2. **TCP State-Exhaustion Attacks**: These attacks attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls, and the application servers themselves. They can take down even high-capacity devices capable of maintaining state on millions of connections.

3. **Application-Layer Attacks**: These target some aspect of an application or service at the Application-Layer. They are the most sophisticated, stealthy attacks because they can be very effective with as few as one attacking machine generating a low traffic rate. This makes these attacks very difficult to proactively detect with traditional flow-based monitoring solutions. To effectively detect and mitigate this type of attack in real time, it is necessary to deploy an in-line or other packet-based component to your DDoS defense.

E. Current Attack Targets and Threat Vectors

Current Attack Targets and Threat Vectors that effect the Communications Sector include, but are not limited to:

- ***Higher Magnitude and Application-Layer DDoS Attacks***: Reported attacks ranging from 309Gbps at the top end through 200Gbps, 191Gbps, 152Gbps, 130Gbps and 100Gbps. Attackers do seem to have been resorting to large, volumetric DDoS attacks to achieve their goals.

- ***Application-layer Attacks***: Have been trending up for several years. However, HTTP POST floods becoming much more common. Although HTTP traffic is still the number one DDoS target, there has been strong growth in application-layer attacks targeting encrypted Web services (HTTPS).

- ***Corporate/Gov't Agency Network Threats***: Advanced persistent threats (APT) are increasingly common, along with growing numbers of attacks targeting BYOD/mobility environments.

- ***Data Center Attacks***: Data centers have become a magnet for DDoS activity, because they represent a target-rich environment. Shared network and data communications infrastructure brings an inherent risk of collateral damage if not properly protected.

- ***DNS Attacks***: The number of high-profile DNS reflection/amplification attacks seen has risen dramatically. The most notorious of these attacks targeted Spamhaus and tipped the scales at over 300Gbps.[122] Many attackers took note and followed suit with their own DNS reflection/amplification campaigns.

[122] *See* Alan McLean, *How the Cyberattack on Spamhaus Unfolded*, http://www.nytimes.com/interactive/2013/03/30/technology/how-the-cyberattack-on-spamhaus-unfolded.html?_r=1& (last visited Mar. 13, 2015).

- ***Mobile Attacks***: Most global and national wireless network operators, still operate traditional GSM, 2G, and 3G networks. However, LTE deployments continue to increase. In the mobility threat landscape, over 90% of all attacks, target the Android operating system and corrsponding mobile apps.

- ***IPv6***: The volume of IPv6 traffic on the Internet appears to be growing very rapidly. However, attackers have learned to exploit vulnerabilties in networks where a dual IPv4 and IPv6 stack is in use by a network operator.

VI. ANALYSIS

The large number of findings highlighted above, reflect threats against critical infrastructure generally, as well as threat elements more closely associated with communication sector assets. In short, the findings above cut across all four layers of the TCP/IP communications model: Application, Transport, Internet, and Network Access (Link) layers. The focus of this sub-group, however, is on the protecting the core infrastructure and assuring network availability, integrity, and confidentiality.[123]

There are a large number of sources for threat information: ISACs, the NCCIC/USCERT/NCC, Cyber-Threat vendors, Think-tanks, News Agencies, and Industry Peers, among others. The NIST CSF emphasizes that "organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances"[124]. However, the NIST CSF also notes that, " the organization may seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events".[125]

A. Community Threat Model / Information Sharing and Analysis:

Network Service Providers within the Communications Sector have a long history of mutual aid and collaboration with each other to respond to major physical events. Many network service provicers are members of the oldest Information Sharing and Analysis Center, the DHS National Coordinating Center, which was created and established more than 30 years ago -- at the request of Industry. Many providers also participate in bilateral or closed trust groups to address core infrastructure security and reliability issues. Notwithstanding these well established venues, some network service providers are taking some incremental, first-steps toward developing more robust protocols for mutual cyber-aid in defending core networks. CSRIC WG4 notes, however, that these first-steps toward mutual aid and support are hampered by lack of legislative clarity surrounding 1) the ability to share cyber-related information; 2) whether action taken either individually or collectively by the providers would lead to greater liability exposure than not taking those actions; and 3)

[123] *See* Section I.
[124] *See* National Institute for Standards and Technology, *Framework for Improving Cybersecurity*, 79 FR 9167 (Feb. 18, 2014) [hereinafter *NIST CSF*], *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[125] *Id*. at 14.

whether there is greater liability exposure when no action is taken individually or collectively by providers.

Nonetheless, there could be clear benefits associated with a "community first" approach toward protecting the core infrastructure, especially when the collaboration and pooling of threat information might validate real-time threats or potential consequences. It could also provide a way to ensure a consistent view of threat information across the sector, enabling the ability to compare defensive decisions, or alternatively for peering partners to mutually support each other.

A community model for information sharing and analysis is consistent with the creation of sector-specific ISACs under PDD63 and this same community-model approach was reaffirmed in the recent Presidential Executive Order[126]. Such venues focus on the needs and commonalities of the community, and must be highly adaptive to address the rapidly evolving threat environment. In this modern era of very rapid information flow and changes in adversary techniques and tradecraft, there is a need to create a shareable, ongoing process to support the security decision-making of core network operators and the broader cyber ecosystem.

As such, the Threat Communications subgroup recommends that Sector members should leverage the threat intelligence capabilities of the Communications ISAC[127] as well as other intelligence sources, and consider participation in both active and trusted community threat venues. Through the Comm-ISAC venue, communication sector members could work to enhance the cyber-related protocols associated with assessing threat, risk, mitigations, and mutual support. This network provider community could collaborate to: identify threat or attack information with a specific focus on core networks; identify relevant "crossover" (between core and enterprise networks) issues to be shared with relevant stakeholders (e.g., exploitation of commercial switching gear, protocol attacks with relevance to core network operators.); or support core network operators through collection of useful resources, case studies, etc., that assist in assessing risk, and choosing defensive-protective options.

With this approach, the Communications Sector can create a more robust process that leverages an existing community-supported and vetted process, and fine tunes it for our segment's specific operational environment, while minimizing cost and duplication.

Using the outputs from such a community threat model and from their own enterprise threat intelligence gathering and analysis, an individual organization can then ask and answer the following questions, to decide on actions it needs to undertake to address a current or pending threat:

[126] *See EO 13691*.
[127] *See* Department of Homeland Security, *National Coordinating Center for Communications*, http://www.dhs.gov/national-coordinating-center-communications (last visited Mar. 13, 2015).

- *Have we gathered the latest threat information from all of the available threat sources like; the ISACs, the NCCIC/USCERT/NCC, Cyber-Threat vendors and Think-tanks, various news agencies and cooperative industry peers?*

- *Were any of our assets affected by these threats?*

- *If yes, what assets, addresses, ports, circuits, servers, switches etc. were affected by these threats?*

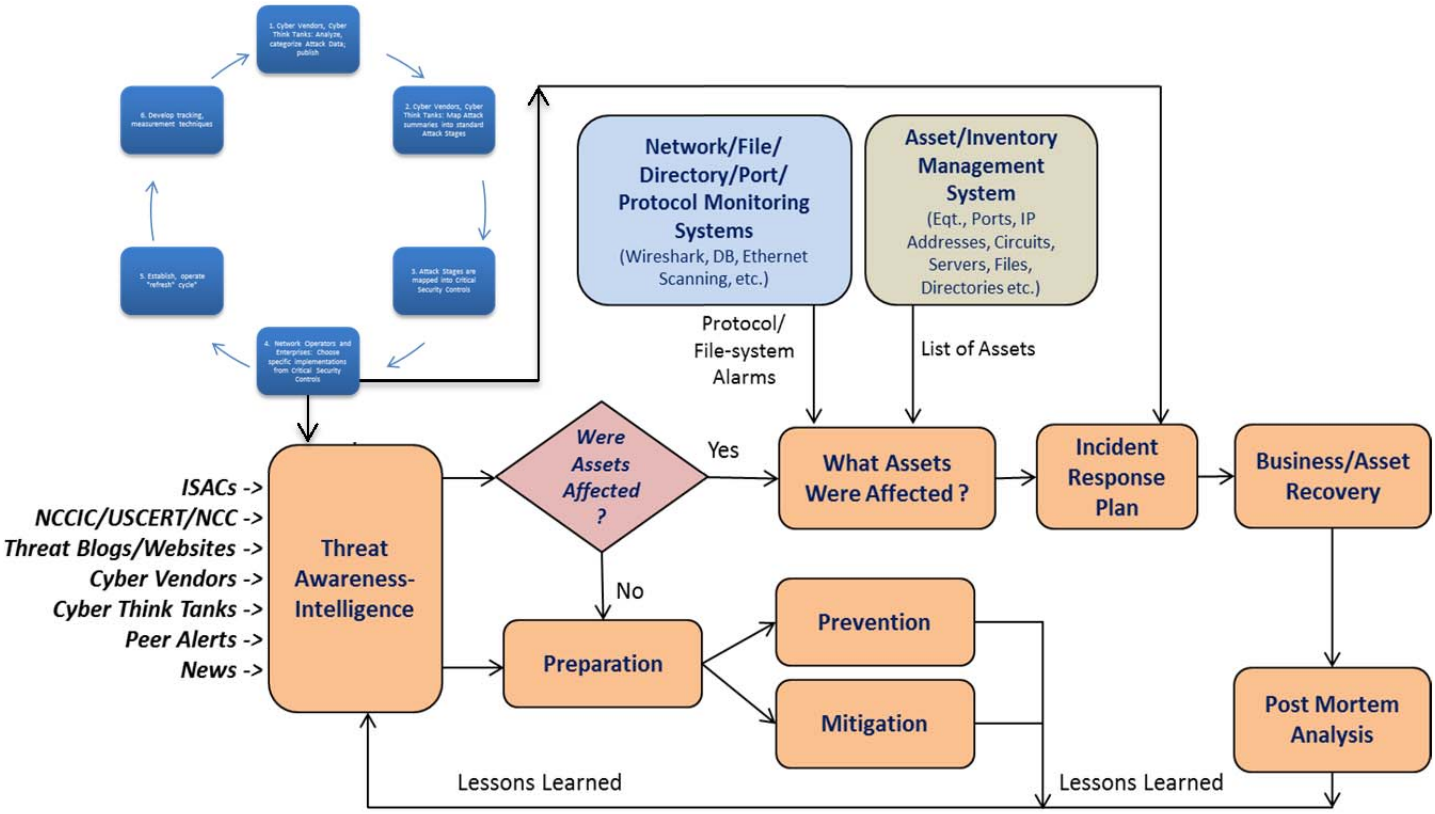
- *If yes, what security controls should we implement to address these threats?*

- *If No, what can our organization do to prevent and mitigate the effects of these threats?*

- *Following our response and recovery actions, what "lessons learned" can we add to our overall threat intelligence?*

The threats feeder group recommends that network operators within the communications sector share the threat intelligence information derived from the questions above with their peers (consistent with applicable laws), thus enabling more efficient and scalable threat information gathering for use in threat analyses and cyber risk management decision making.

Illustrative Threat Intelligence / Information Sharing Process Model:



VII. CONCLUSIONS AND RECOMMENDATIONS

- The community threat models and threat intelligence handling models for threat awareness that are described in this report must continually evolve in order to respond to the ever changing tactics utilized by malicious actors and the unknown threats of tomorrow. Tailored threat knowledge can be used to better defend our networks.

- The threats feeder group concludes that the current and future threat landscape will continue to evolve and will require agile and adaptive methods of obtaining threat intelligence, in order to adequately protect critical communications infrastructure.

- The threats feeder group concludes that organizations should continuously gather Threat Intelligence from a multitude of industry and government agencies, and cyber threat think-tanks in order to stay ahead of malicious actors and attackers and adequately protect critical communications infrastructure.

- The threats feeder group recommends that a community model for threat intelligence or information sharing and analysis be considered by organizations intending to use threat intelligence in their quest to protect critical infrastructure and protect critical data from future-unknown cyber threats.

- The threats feeder group recommends that Sector members should leverage the threat intelligence capabilities of the Communications ISAC (Comm-ISAC) as well as other intelligence sources, and consider participation in active and trusted community threat venues.

- The threats feeder group recommends that network operators within the communications sector share threat intelligence information with their peers (consistent with applicable laws), thus enabling more efficient and scalable threat information gathering for use in threat analyses and cyber risk management decision making.

VIII. ACKNOWLEDGEMENTS

The following industry and government reports were utilized by the threats feeder Group during the analysis portion of generating this report:

NSIE 2014 Risk Assessment

Verizon: 2014 Data Breach Investigations Report
https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf

Websense 2014 Threat Report
http://www.websense.com/assets/reports/report-2014-threat-report-en.pdf

Symantec: Internet Security Threat Report
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Sophos: Security Threat Report 2014, Smarter, Shadier, Stealthier Malware
http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

Cisco's 2014 Annual Security Report
http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

Hewlett Packard: Cyber risk report 2013
http://www8.hp.com/h20195/v2/GetPDF.aspx%2F4AA5-0858ENW.pdf

Department of Homeland Security: Executive Order 13636: Improving Critical Infrastructure Cybersecurity
https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

EY: Under Cyber Attack – EY's Global Information Security Survey 2013
http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf

Bipartisan Policy Center: Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat
http://bipartisanpolicy.org/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf

Booz Allen: Cyber Power Index
http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

Office of Management and Budget: Annual Report to Congress – Federal Information Security Management

Arbor Annual Threat Report focused on Denial of Service
http://www.arbornetworks.com/resources/infrastructure-security-report

Ponemon Institute Exposing the Cybersecurity Cracks: A Global Perspective
http://insidecybersecurity.com//index.php?option=com_iwpfile&file=jul2014/cs07172014_Report_Ponemon_2014_Part2.pdf

CSRIC IV WG5 "Remediation of Server-Based DDoS Attacks" Final Report
http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_%28pdf%29_V11.pdf

Guide to Cyber Threat Information Sharing (Draft), NIST Special Publication 800-150 (Draft)

http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf