Before the
National Institute of Standards and Technology
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of)
)
Developing a Framework to Improve) Docket No. 130208119-3119-01
Critical Infrastructure Cybersecurity)

COMMENTS OF
THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

Howard J. Symons
Christopher J. Harvie
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo
701 Pennsylvania Avenue, NW
Washington, DC 20004

April 8, 2013

Rick Chessen
Loretta Polk
Stephanie L. Podey
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW 1

I. CURRENT RISK MANAGEMENT PRACTICES IN THE CABLE INDUSTRY 4

II. CABLE COMPANIES' USE OF FRAMEWORKS, STANDARDS, GUIDELINES, AND BEST PRACTICES....................9

A. Cable Industry Participation in Multi-Stakeholder Groups and Utilization of Existing Cyber Resources....................10

B. Cable Company Cyber Practices and Policies 12

C. Cable Operators to Minimize Cyber Threats That May Originate From End-User Equipment 17

III. RECOMMENDATIONS REGARDING STRUCTURE AND OPERATION OF FRAMEWORK....................19

A. The Cybersecurity Framework Must Be Flexible and Embrace Diversity....................19

B. The Cybersecurity Framework Should Include All Relevant Industry Sectors 21

C. The Cybersecurity Framework Should Draw on Existing Resources and Rely on Industry-Driven Solutions to Address New Vulnerabilities and Changes to the Threat Landscape....................23

CONCLUSION....................25

Before the
National Institute of Standards and Technology
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
Developing a Framework to Improve Critical Infrastructure Cybersecurity	))	Docket No. 130208119-3119-01

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association (NCTA)[1] hereby submits its comments in response to the Request for Information (RFI)[2] issued by the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce in the above-captioned proceeding.

INTRODUCTION AND OVERVIEW

As the nation's largest providers of broadband Internet access service, NCTA's member companies have been at the forefront of developing and implementing a broad range of practices and protocols for identifying and addressing cybersecurity risks and vulnerabilities. Cable companies work every day to assess, deter, and neutralize network security vulnerabilities and threats. In so doing, they have incorporated a range of recognized industry standards and measures into their cybersecurity practices and protocols.

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing $200 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 26 million customers.

[2] Department of Commerce, National Institute of Standards and Technology, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Docket No. 130208119-3119-01, 78 Fed. Reg. 13024 (Feb. 26, 2013) ("RFI").

This experience teaches that to be effective, the Cybersecurity Framework must reflect the dynamic nature of cyber threats. The threat landscape is constantly evolving, as cyber criminals develop new methods to overcome existing security measures. Indeed, cyber criminals study remediation technology and tools to test and implement new techniques for penetrating networks and evading detection. They use the latest software tools and technology at the same time that they are used for legitimate purposes. Accordingly, it is critically important to develop a Cybersecurity Framework that is flexible, agile, and adaptable, and recognizes that diversity is preferable to uniformity. It should offer a broad menu of recommended options and practices that are outcome-oriented, rather than prescriptive.

The Framework must allow for continued innovation and modification to reflect the constantly-changing threat landscape, and it must be sufficiently flexible so that companies can adapt and customize recommendations to reflect their specific network architecture, business operations, and existing cybersecurity protocols and processes. Our cyber defense posture is best served by policies that promote a flexible solutions-oriented process that builds on existing industry collaborations and encourages experimentation, while avoiding a constrictive one-size-fits-all, top-down approach that mandates conformity with prescriptive measures that are bound to become obsolete over time.

In that regard, cable operators and others in the communications sector with extensive cybersecurity expertise should be permitted to continue with their current efforts, rather than having to divert capital and resources away from these efforts toward mandates that differ from practices and protocols that they have already implemented. If there are gaps whereby new or emerging threats may not be addressed by an existing industry practice, those gaps should be filled in the first instance by giving industry the opportunity to develop responses through the various industry and multi-stakeholder groups that are already at the forefront of cybersecurity development and innovation. NIST should not assume that any gaps it may identify in developing the Framework must be filled by government-imposed standards or practices.

It is also essential that the Framework be adaptable to differences both across and within industry sectors. No single isolated set of standards or industry best practices suffices to meet the needs of today's complex cyber environment. Rather than establishing a collection of sector-specific practices, the Framework should instead identify leading consensus standards and industry best practices that could be adapted by particular sectors and entities and be tailored to their unique circumstances. For example, the standards and practices that comprise the Framework should take into account differences in the design, size, and complexity of a particular company's network architecture and business model and provide flexibility in how an affected entity protects against cyber threats. It should be technology-neutral and cost-effective, and should not interfere with companies' ability to provide high quality service to customers.

More broadly, the Framework should recognize that ***all*** industry sectors have a responsibility to address cybersecurity vulnerabilities in their critical infrastructure. In light of the interdependent nature of the Internet, it would be unreasonable and ineffective to impose a disproportionate burden on the communications sector to mitigate the multitude of risks from other sectors. Although the Presidential Policy Directive identifies communications systems as "uniquely critical due to the enabling functions they provide across all critical infrastructure sectors,"[3] the vast majority of cyber threats originate from outside communications systems. Most cyber threats relate to vulnerabilities that exist not at the network level, but at end-user

[3] Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

access points and Internet-facing devices susceptible to compromise. Thus, the Framework should establish the expectation that stakeholders from all industry sectors will take the steps necessary to secure their own systems and data. NIST should likewise recognize that Information Technology (IT) products and services play a critical role in addressing cybersecurity vulnerabilities, and their exclusion from the Framework will leave many critical issues unaddressed.

Finally, the adoption of the Framework and other cybersecurity measures would be enhanced by the adoption of liability protections for private entities that employ cyber defense tools and techniques. Such protections would minimize litigation risk and other legal uncertainties from the use of such measures. Clear legal authorization to share cyber threat information among private actors and between the private sector and the government would facilitate the detection and deterrence of these threats and the development of new practices and protocols to combat them. While these issues are outside the scope of this proceeding, they must be addressed as part of the government's overall cybersecurity policy.

These comments provide an overview of the type of practices, tools, and protocols that NCTA's member companies utilize in as part of their ongoing efforts to secure their networks against cyber threats and vulnerabilities. Against the backdrop of this experience, we next offer recommendations for the "methodologies, procedures, and processes"[4] that should be included in the Cybersecurity Framework – as well as those that should be avoided.

I. CURRENT RISK MANAGEMENT PRACTICES IN THE CABLE INDUSTRY

For providers of broadband Internet access services, the public interest in securing critical infrastructure from cyber attacks aligns with companies' business interests in providing secure

[4] *Id.* at 13025 (quoting Executive Order 13636-Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 19, 2013) ("Cybersecurity EO")).

networks to meet customer demand. Cable companies have strong, market-based incentives to address cyber threats and vulnerabilities and incorporate the cybersecurity practices and protocols into their business operations. Because our companies' business success depends upon customers using our networks and consuming our network-based offerings, ensuring a safe and secure network environment is a top business priority. Thus, cable companies devote substantial capital, resources, and manpower to preventing, detecting, deterring, and responding to cybersecurity threats, notwithstanding the absence of any express government directive to do so. Securing our networks against cyber threats is a business imperative for the communications industry.

Broadband providers' experience in cyber risk management has shown that any risk management approach must recognize the enormous diversity of challenges faced by the various critical infrastructure sectors. Each sector, and indeed each entity within any given sector, faces its own unique cyber threats and risk profiles. Accordingly, even "best" practices, standards, and tools may not be appropriate – and could even be counter-productive – for some entities or sectors, depending upon the risk profiles they face. Organizations should be encouraged to address cyber threats within their own unique risk management processes, with an eye towards the impact and relevance of a given threat on their individual systems.

The RFI notes that the "national and economic security of the United States depends on the reliable functioning of critical infrastructure, which has become increasingly dependent on information technology."[5] But dependence on information technology should not be an excuse to fob off disproportionate cybersecurity responsibilities on owners and operators of communications networks.

[5] RFI at 13025.

Cyber threats pose a particular risk to information systems that supply critical key resources for the nation: water supply, nuclear power plants, electricity grids, financial networks.[6] These are key commercial networks whose disruption could be especially problematic for the nation.[7] Thus, our companies recognize that elements of their networks could be subject to the Framework under consideration to the extent that they support the reliable functioning of these types of entities, as well as other owners and operators of critical infrastructure. At the same time, however, communications infrastructure and services include a wide array of non-critical assets and functions, so the determination of what constitutes "critical infrastructure" should be made on a granular basis to avoid sweeping in non-critical elements. Further, it is the owners and operators of such critical infrastructure, not owners or operators of communications networks, who must bear the ultimate responsibility of ensuring that their own internal systems and data are secure.

Broadband service providers, such as cable companies, treat cybersecurity as a central component of their overarching enterprise risk management strategy. Enterprise security risk management processes aim to decide how to identify, deter and mitigate security risks. Overarching principles of cable's risk management practices include continuous oversight and monitoring of facilities and assets that present potential security vulnerabilities; prioritizing risks and threats in light of deterrence capabilities and remediation tools and strategies; responding to

[6] *See e.g.,* 42 U.S.C. 5195c(e) (defining critical infrastructure 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").

[7] In contrast, residential networks providing access to the Internet – while serving many people – do not necessarily implicate distribution of key resources, and temporary incapacity of such network facilities, while inconvenient, would not ineluctably "have a debilitating impact on security, national economic security, national public health or safety." Cybersecurity EO at 11739. It makes sense for the government to prioritize its cybersecurity efforts to protect delivery of key resources, and cybersecurity policy should be tailored to addressing those priorities.

and mitigating threats and intrusion attempts; and reassessing risks, strategies, and tools in light of such threats and intrusion attempts.

The effort to promote and enhance cybersecurity is not just a matter of acquiring and deploying the correct technological tools, it also is an organizational and managerial undertaking. Cable broadband providers have put in place cross-function internal processes for examining cyber risks to facilitate the full and detailed integration of security risk management into corporate processes at every level of operation. They have established designated teams or cyber committees with representatives from key areas of the company, such as risk management and governance, security, privacy, engineering, legal, network operations, and government relations. This approach enables them to combine insights from a variety of functionalities to examine information security and risk management principles from multiple perspectives.

These cybersecurity teams or groups meet on a regular basis to provide strategic oversight in policy, leading practices, maintaining and driving consistency in strategic relationships in both government and industry, reviewing potential "What If…" analyses arising from current events or risks, and sponsoring live cybersecurity exercises. A designated corporate focal point for cyber issues can also coordinate cybersecurity efforts and initiatives, review and update a company's protocols and response plans, establish and maintain relationships with appropriate government agencies, review metrics, and keep abreast of best practices. It also facilitates the flow of information to senior management and the board of directors, as well as to each functional area, ensuring that security policies, cybersecurity activities, and related programs are coordinated across the company, and that the company maintains relationships with relevant third party and government organizations.

Cable companies also draw upon external resources in connection with their cybersecurity risk management efforts, including such widely-accepted international risk management practices from OCTAVE Allegro, COSO and COBIT, ISO/IEC 31000:2009, ISO/IEC 27005, and Factor Analysis of Information Risk (FAIR). Although most policies and best practices have been developed internally (informed by companies' unique expertise and experiences and designed to protect their particular network architecture and business operations) cable companies also routinely engage with consulting partners to review, refine, and update existing practices as needed. The companies also collaborate with vendors, equipment providers, and security management services to develop and integrate new innovations.

While cable companies have successfully developed and maintained unique cybersecurity practices and protocols on their own initiative and without government mandates, their work has been informed by input and guidance from appropriate Federal government officials and agencies. In particular, the cable industry works with the Department of Homeland Security (DHS) through the Communications Sector Coordinating Council (CSCC). The CSCC coordinates initiatives to improve the physical security and cybersecurity of sector assets; to ease the flow of information within the sector, across sectors, and with designated Federal agencies; to address issues related to response and recovery under all hazards to assure the continued operation of vital communications services; and to develop and implement the Communications Sector-Specific Plan (CSSP) as required by the National Infrastructure Protection Plan (NIPP). The CSCC's expertise and experience make it the most logical and appropriate focal point for government-coordinated efforts on cybersecurity, including with respect to the development of the Framework.[8]

[8] Government coordination is crucial to ensure that private sector cybersecurity resources are not strained through duplicative, overlapping efforts, particularly for industry security and technical experts.

In addition to its work with the CSCC, the cable industry has enhanced its ability to create best practices for risk management in general, as well as to identify and address cyber-specific issues and threats through its voluntary participation in Federal initiatives such as the National Cybersecurity and Communications Integration Center (NCCIC), which is comprised of the United States Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC)/ Communications Information Sharing and Analysis Center (COMM ISAC), and the Federal Bureau of Investigation's Infragard, to name just a few. Cable companies also partner at the local and state levels with law enforcement and emergency management agencies, in particular, by holding seats in Emergency Operation Centers (EOCs).

II. CABLE COMPANIES' USE OF FRAMEWORKS, STANDARDS, GUIDELINES, AND BEST PRACTICES

Within the communications and information technology sectors, there are a number of existing organizations dedicated to developing cyber security best practices. NCTA and its members have been actively involved in Federal public-private partnerships and industry groups dedicated to improving the security and resiliency of critical communications infrastructure against cyber threats. The collaborative multi-stakeholder approach embraced by the communications and information technology industries has led to the creation and development of a wide variety of standards and practices that cable companies have been able to adapt and implement while maintaining the flexibility needed to address their individual needs.

The standards discussed in this section serve as reference points that can be adapted in developing system-specific best practices. It would be unrealistic and counterproductive, however, to expect any entity to adopt in full any particular framework or set of standards that is developed for general implementation without accounting for the entity's specific technical and business requirements. Indeed, it is inevitable that some elements of any given framework will be inappropriate for an organization's specific network architecture and business practices.

A. Cable Industry Participation in Multi-Stakeholder Groups and Utilization of Existing Cyber Resources

Cable companies participate in a number of industry working groups that develop standards and best practices to address cybersecurity issues. For example:

- **Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)** - M^{3}AAWG's membership includes cable companies and other broadband Internet access providers as well as software companies, network equipment vendors, and other technology companies. M^{3}AAWG has published best practices for a variety of cyber issues, including *Best Practices to Address Online and Mobile Threats* and *Best Practices for Implementing DKIM to Avoid Key Length Vulnerability*.[9]

- **North American Network Operators Group (NANOG)** - NANOG is an educational and operational forum for the coordination and dissemination of technical information related to backbone/enterprise networking technologies and operational practices. NANOG's Best Current Operating Practices Working Group is dedicated to producing documented best practices "for engineers by engineers."[10]

- **Domain Name System Operations Analysis and Research Center (DNS-OARC)** - DNS-OARC brings together key operators, implementers, and researchers to coordinate responses to attacks and recommends best current practices for mitigating DNS Denial of Service attacks.[11]

- **Broadband Internet Technical Advisory Group (BITAG)** - BITAG is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists to develop consensus on broadband network management practices and other technical issues.[12]

- **Cable Television Laboratories, Inc. (CableLabs)** - CableLabs is a non-profit research and development consortium that is dedicated to pursuing new cable telecommunications technologies and to helping its cable operator members integrate those technical advancements into their business objectives. CableLabs serves the cable television industry by: researching and identifying innovative broadband technologies; authoring specifications, including security specifications for the

[9] http://www.maawg.org/published-documents.

[10] http://www.nanog.org/meetings/nanog57/abstracts.php?pt=MjA1MyZuYW5vZzU3&nm=nanog57.

[11] https://www.dns-oarc.net/wiki/mitigating-dns-denial-of-service-attacks.

[12] http://www.bitag.org/index.php.

DOCSIS and PacketCable platforms; conducting certification and qualification testing of products; and disseminating information.[13]

- **The Society of Cable Telecommunications Engineers (SCTE)** - SCTE is a non-profit professional association that provides technical leadership for the telecommunications industry and serves its members through professional development, standards, certification and information. The Data Standards Subcommittee of SCTE's Engineering Committee has published ANSI/SCTE 135-3 2013 standards to secure DOSCIS 3.0 platforms.[14]

- **ISACA** - ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA offers a number of governance, security, and audit frameworks designed specifically for enterprises that use information systems.[15]

In addition to employing standards and best practices developed by these organizations, cable operators participate in the work of other relevant groups, including the International Organization of Standards (ISO), National Security Information Exchanges (NSIE), USTA Communications Industry Security Controls Working Group (CISCWG), Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC), and IEEE Committee for Quality and Reliability. And they have successfully adapted a range of consensus standards and best practices to fit their individual requirements. These include the NIST 800-53 and 800-37 cyber security best practices, SANS Institute's Twenty Critical Security Controls, the ISO 31000 series of guidelines and principles for general risk management, and the ISO/IEC 27000 series best practice recommendations on information security management, risks and controls. As noted above, the cable industry also participates in the CSCC public-private partnership under DHS, and collaborates with other government entities to identify practices and measures for addressing a wide variety of cybersecurity issues.

[13] http://www.cablelabs.com/about/.

[14] http://www.scte.org/standards/Standards_Available.aspx.

[15] http://www.isaca.org/about-isaca/Pages/default.aspx.

Whether the standards and practices are developed through industry-driven or collaborative public-private forums, it is critical to keep in mind that these standards and practices are guidelines that each company must tailor to fit its own particular network and business circumstances. Solutions that are right for one company may not be appropriate for others, even with companies in the same industry, because the relevant factors can vary considerably from company to company. While industry standards can serve an important role in developing effective cybersecurity practices, it is critical to preserve flexibility for each company to implement them in a manner that accords with each company's particular circumstances.

B. Cable Company Cyber Practices and Policies

Cable broadband providers use a variety of tactics and tools to implement existing standards and best practices for cybersecurity risk management, including:

Intrusion Detection and Prevention Systems
Distributed Denial of Service Detection and Mitigation
Firewalls (including WAFs)
Threat Correlation
Data Loss Prevention (DLP)
Security Information and Event Management (SEIM)
Encryption Key Management
AVM/Bot Detection and Remediation
Direct Security Event Surveillance via Security Response Centers
Incident Response Process
Security Auditing Program
Secure Network Design and Engineering
Penetration Testing and Mock Incident Drills
Identity Management/ Role Management
Anti-Virus
Log Collection and Analysis
Vulnerability Detection
System Configuration Change Auditing
Mobile Device Management
Database Activity Monitoring (DAM)
Darknets
Honeypots
Sinkholes
Null0/Null route
Bogon Filtering
Walled Gardens
Intercepting Proxies
Governance, Risk, and Compliance (GRC)
Threat Modeling
Facilitated Risk Assessments
Network Security Monitoring
Spam Filtration

These combined controls provide network level protections; restrict network routing and access; restrict management port access and availability; permit oversight by technologies that are aware of malicious packets, communication, or unusual traffic patterns; and monitor for security and non-security events to confirm continuous availability and health. Key practices, protocols, and tools are discussed in more detail below.

Asset Management and System Segregation. Cable companies view cybersecurity as a key component of enterprise security risk management, and draw upon input from all operational and organizational function areas within the company to identify critical assets that need to be secured against cyber threats, as well as the appropriate individuals or departments responsible for managing each asset. Companies may employ a "zoning model" to differentiate and segregate business and operational systems according to system content and risk.[16] Assets and infrastructure are placed into "zones of implied trust" according to their operational functions and security needs. Location in a given zone depends on an asset's content, access requirements, and risk assessment, and governs the restrictions on that asset's communications. An asset's zone is applied through the assignment of its IP address, which allows a device to browse the network according to its particular zone assignment.

Zoning systems are built around the particular company's standards and policies, and are defined by firewalls and access control lists that protect and further segment critical systems. Network operators use differentiated services to route and isolate traffic packets by service type in order to identify anomalies. Risk-based security governance also helps companies identify the systems that require the greatest levels of security protection and control. Systems with

[16] The separation of business and operational systems may not be appropriate in all circumstances, particularly for smaller providers, or in instances where such segmentation adversely affects network functionality, operational controls, or system usability.

information of higher business value, customer information, or security ramifications can, as appropriate, be given priority in security scanning, penetration testing, and remediation.

Network Resilience and Security Engineering. Companies have implemented a "defense in depth" resiliency strategy, which starts by hardening key network elements with asset-specific security capabilities to create a network stronghold, and then layer external tools and systems on top of those elements to seek out and eliminate threats before they fully materialize. Because each key asset and operating system within a network typically contains its own native defenses and security protocols, companies are able to maintain a standard "secure build" that establishes a baseline level of security to ensure that each device contributes to the network's overall security posture. An operator may then add external tools and measures to monitor network data flows and identify threats. Examples include the purposeful rerouting of traffic to defend against distributed denial of service attacks, intrusion prevention systems for detecting a variety of known threats and analyzing traffic patterns, and individualized tools that seek out specific threats.

Companies take a holistic approach to security, engaging security architects, risk analysts, vulnerability engineers, and penetration testing during all phases of the systems development life-cycle. They also engage in periodic application code reviews to screen for security vulnerabilities and ensure sound security coding practice. Using tools from a variety of vendors to bolster the network's overall security, companies continue to adapt existing security to "agile" development methodologies.

Network Monitoring and Incident Response. To understand threats to network operation centers and management networks, cable companies employ host forensics, host configuration management, network event forensics, network configuration management, and real-time traffic analysis. To deter and mitigate these threats, best practices include using malware scanning and detection, end-point security solutions, root kit detection capability, user authentication, and perimeter protections such as firewalls, intrusion detection and prevention tools, packet collection and perimeter networks.

Cable broadband networks are monitored through security operating centers (SOCs) that are manned by personnel twenty-four hours a day, seven days a week. Security incident and event management tools and systems track alerts that are triggered from security points on the system. Data from network-wide logs and events are then aggregated into a central location where tools with heuristics capabilities analyze the information in order to link issues and develop a consolidated picture of existing threats. Cable operators use a number of third-party vendors and tools to monitor a variety of potential events that may stem from particular sources. Some of those tools include Security Information and Event Management (SIEM) technology, an intrusion prevention system, vulnerability detection, log collection and aggregation, anti-virus software, behavioral analysis to identify previously unknown zero-day malware, system configuration change auditing, mobile device management, and data loss prevention. In addition, those companies with personnel in charge of maintaining security intelligence may access information from the Department of Homeland Security and other Federal agencies, as well as internal intelligence and commercial product intelligence from industry third parties.

SOCs can also serve as focal points for incident response, controlling all activities and acquisition of evidence that are required during the course of an event. When a cyber incident is detected, the SOC may review the event and perform initial triage for incidents identified as low or medium security risks using established playbooks. Incident handling policies and procedures mandate the involvement of representatives from a variety of functional areas within a company, although the exact makeup of an incident response team may depend on which components of the network are at risk. Escalation procedures for high or critical incidents also are typically in place, which are designed to quickly engage appropriate personnel and expertise for purposes of analyzing, containing and eradicating the incident.

Companies maintain "run books" for incident handling policies and procedures that may reflect external guidelines, such as SANS CSC #18 – Incident Response and Management or NIST SP 800-61- Computer Security Incident Handling Guide, but are adapted to a company's particular circumstances. Run books contain protocols for every layer of security, from identification, to eradication, to restoring system services, to capturing evidence for forensics and post-mortem analysis. Policies are regularly reviewed and updated, and companies undergo drills and mock incident exercises to test readiness. These mock incidents allow companies to examine the efficacy of response plans and protocols, and provide insight into whether a real security event might alter the overall security risk analysis.

Encryption and User Access. To combat the theft of identity profiles, cable operators have developed tools and protocols that combine identity and role management systems with encryption and key management tools.[17] Role-based management systems keep track of network permissions for all personnel based on their existing roles and responsibilities, proactively limiting or eliminating access to assets that are no longer relevant in the event of an employee's position change. When appropriate, multi-factor authentication is also used to authenticate a user's access to certain internal systems.

[17] It is important to recognize that while encryption is an effective tool when used properly, it cannot serve as a panacea against all cyber threats. Encrypted data will inevitably need to be used in a clear text format, at which point it will be vulnerable to attack. Furthermore, even when encrypted, such data may be vulnerable to direct attacks against the encryption keys. While encryption is appropriate in many circumstances, it is not technically feasible or economical to use it everywhere or for all data.

Cable operators also use a wide variety of encryption and key management tactics throughout network infrastructure, including DOCSIS 3.x encryption between the cable modem termination system and capable customer-premises equipment, Virtual Private Network encrypted tunnels for third party connectivity, Secure Sockets Layer encryption for web presence authentication, laptop whole-disk encryption, code signing, and targeted encryption for data at rest. Every encryption type has its own methodology, which adds individual layers of security to the network as a whole.

Privacy and Civil Liberties Protections. The cable industry is subject to myriad international, Federal, state, and contractual requirements related to privacy and data security that restricts how, what, and when we can collect, use, and disclose customer information. Thus, the industry has developed a number of privacy and civil liberties protections. Unlike governmental bodies, cable operators have a direct and voluntary business relationship with our customers. This relationship – and the concomitant need to ensure our subscriber's trust – is fundamental to our business success, and therefore guides decision-making about how to build, structure, and defend our services against cyber threats.

C. Cable Operators to Minimize Cyber Threats That May Originate From End-User Equipment

While the Cybersecurity Framework is intended to secure and protect critical infrastructure from cyber threats, it is important to bear in mind that such threats rarely exclusively originate from within systems maintained by the network operator. End-users, whether they are residential customers or complex organizations that operate critical infrastructure themselves, are an integral part of the Internet's "network of networks." As such, they can serve as the launching pad for distributed targeted attacks on the entire infrastructure. Botnets are particularly insidious because they turn ordinary users into unwitting participants in criminal enterprises by allowing malefactors to take control of a user's device for their own nefarious purposes. Thus, a botted device can cause significant harm to both the individual user and to the entire network and beyond.

Recognizing the risks that can originate from consumer equipment, cable operators have developed consumer-based security tools that work in conjunction with network-based measures to help safeguard end users from botnet threats by enabling them to protect their computers and mobile devices from cyber-attacks and loss or corruption of data. The tools typically include security software from nationally known vendors like Norton, McAfee, and F-Secure; anti-phishing and anti-spyware technology; identity protection; anti-botnet and anti-virus tools; and a consumer education program. Many operators provide these host-based security tools to each residential broadband customer at no additional expense.

The well-established nature of these consumer-facing programs demonstrates that providers already have strong incentives to deploy them without the need for government involvement. Thus, these tools would complement the Cybersecurity Framework but would not need to be part of the Framework, which should focus on protocols, methodologies, procedures, and processes to address cyber risks in critical infrastructure.

In addition to deploying tools to help deter cyber threats that may originate from the network edge, cable operators have actively participated in the Administration's Botnet Initiative, which provides a model for the broad-based participation of information technology vendors in developing key cybersecurity principles. The Botnet Initiative grew out of an earlier Request for Information (RFI), jointly published by the Department of Homeland Security and the Department of Commerce, on the creation of a voluntary industry code of conduct to address the detection, notification, and mitigation of botnets.[18] Critically, this initiative has involved the participation and engagement of all segments of the Internet ecosystem, including search engines, security tool vendors, and applications providers. Cable companies have also played a leading role in the FCC's CSRIC Working Group 7, which recently developed an Anti-Botnet Code of Conduct.[19] Consumer-facing botnet deterrence programs will benefit from these efforts.

III. RECOMMENDATIONS REGARDING STRUCTURE AND OPERATION OF FRAMEWORK

Over the past decade, the cable industry has been operating on the frontlines against cyber threats, investing in systems and personnel to prevent, detect, deter, and respond to cybersecurity threats. They have independently developed effective procedures and protocols to secure all components of their broadband network, including those that support critical infrastructure. The cable industry's experience demonstrates that to be effective, the Cybersecurity Framework must be embody three core characteristics: it must be flexible, it must include all relevant industry sectors, and it must draw on existing resources and rely on industry-driven solutions to address new and emerging threats.

A. The Cybersecurity Framework Must Be Flexible and Embrace Diversity

Cyber criminals are constantly innovating, thereby necessitating a Framework founded on flexibility – rather than prescriptive rules – so that companies can adapt and avail themselves of the growing and changing array of technologies, solutions, and counter-measures that are

[18] Department of Commerce, National Institute of Standards and Technology, National Telecommunications and Information Administration; Department of Homeland Security, *Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware,* Docket No. 110829543-1541-01.

[19] CSRIC III WG7: Botnet Remediation, Final Report, *U.S. Anti-Bot Code of Conduct (ABC) for Internet Service Providers (ISPs): Barrier and Metric Considerations* (March 2013), *available at* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf; *see also* http://www.maawg.org/abcs-for-ISP-code.

available. Compliance with the Framework should not be based upon adherence to standards that may quickly become obsolete. Because of the dynamic and constantly-changing nature of cyber threats, compliance with a particular set of standards is not necessarily tantamount to actual security. Accordingly, if any "conformity assessment" inquiry is deemed necessary or appropriate, it should not entail rote examination of how well an entity or sector is implementing certain practices. Instead, the assessment should focus on how secure an entity's networks are and how capable that entity is of quickly detecting and neutralizing new vulnerabilities and unknown threats. Indeed, extensive government auditing and oversight of compliance with restrictive standards (that might include directives on training, certification, or technologies) would be counter-productive, shifting companies' focus away from detecting and deterring the latest iteration of cyber threats and toward checklist compliance with rapidly obsolescing standards.

Addressing network vulnerabilities and deterring cyber threats is akin to an arms race. As new threat methods are utilized and then discovered and addressed, cyber criminals and other bad actors looking to penetrate networks make modifications to elude detection. Indeed, cyber criminals regularly study and deploy remediation technology to test and implement new evasion techniques. Much of the current malware is developed using the most up-to-date legitimate software developments, such as Software as a Service (SAAS). Accordingly, the Cybersecurity Framework should recognize that diversity and flexibility is preferable to uniformity.

A multiplicity of cyber security solutions also limits the negative impact if one solution is compromised, reducing potential vulnerability. By contrast, mandating a specific strategy to combat cybercrime would provide a roadmap that enables cybercriminals to navigate their way around such standardized defensive measures. Cyber attacks will be harder to initiate or perpetuate where the attacker is forced to confront different strategies and tools from a variety of service providers and vendors. As evidenced by the takedown of the DNS Changer botnet in the FBI-led Operation Ghostclick, the element of surprise and an unanticipated response by the security community (public and private) is critical and effective in the global battle against cybercrime.[20] By embracing flexibility and diversity, the Cybersecurity Framework will encourage critical infrastructure owners and operators to adopt the kind of complex and multi-layered cyber defenses that are more likely to withstand a sophisticated cyber attack.

B. The Cybersecurity Framework Should Include All Relevant Industry Sectors

The communications sector has taken a central role in developing cybersecurity systems that protect critical infrastructure. According to DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), nearly 60 percent of all cyber incidents reported in fiscal year 2012 occurred in the energy, dams, water, and nuclear sectors.[21] Another 11 percent originated from Internet facing control system devices susceptible to compromise. ICS-CERT reports that many critical infrastructure assets are directly facing the Internet, and in some instances have weak, default, or nonexistent logon credential requirements, which leave the systems vulnerable to attack.[22] Meanwhile, only two percent of cyber incidents came out of the

[20] *See* Fed. Bureau of Investigation, *Operation Ghost Click*, *International Cyber Ring That Infected Millions of Computers Dismantled* (Nov. 9, 2011) ("A complex international investigation such as Operation Ghost Click could only have been successful through the strong working relationships between law enforcement, private industry, and our international partners."), *available at* http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911.

[21] *See* ICS-CERT Monitor, Q42012, at 5, *available at* http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf ("*ICS-Cert Monitor*").

[22] *Id.* at 4.

communications sector, less than sectors such as critical manufacturing, commercial, chemical, transportation, health care, and government.[23]

An effective cybersecurity defense must therefore include the active participation of all industry sectors, including the IT sector. As noted above, the RFI states that our nation's national and economic security depend on the reliable functioning of critical infrastructure, which is increasingly dependent on IT. But such dependence should not be the basis for imposing disproportionately more cybersecurity responsibilities on owners and operators of communications networks. To the extent that some sectors are regarded as uniquely critical to the fight against cyber threats and vulnerabilities, it is possible that those industry sectors are already demonstrably further along with the task of developing and incorporating best practices and protocols. Industry sectors that have been facing these issues for a long time may not require as much regulatory guidance as those sectors that are just beginning to address cybersecurity. Moreover, the type of network-based security that broadband providers work continuously to provide cannot, by itself, protect against cyber threats that exploit insecure Internet access points under the control of other critical industry sectors.

NIST should avoid peremptorily determining that certain entities should be excluded from the Framework. For instance, IT products and services are critical elements of the broadband ecosystem and represent gateways through which cyber threats can enter that ecosystem. In fact, each of the top ten IT companies reported dozens of distinct vulnerabilities in a single three-month period last year.[24] ICS-CERT also found that almost half of identified cyber vulnerabilities appeared to relate to inherent flaws in the IT hardware/software solution or

[23] *Id.* at 5.

[24] TrendMicro, "Top Malicious Top Ten," *available at* http://www.trendmicro.com/us/security-intelligence/current-threat-activity/malicious-top-ten/index.html.

deficiencies best addressed by the original IT service provider.[25] Broadband infrastructure also includes content delivery networks (CDNs), server farms, and services operated by entities such as Google, Facebook, Yahoo, and others. All sectors rely on these facilities and services, which in turn rely on IT products and services. Vulnerabilities and cyber threats may be found at any layer of the Internet or in relation to any product. It is therefore necessary and appropriate that these entities are part of Cybersecurity Framework.

C. The Cybersecurity Framework Should Draw on Existing Resources and Rely on Industry-Driven Solutions to Address New Vulnerabilities and Changes to the Threat Landscape

As discussed above, there is a wide variety of ongoing cybersecurity initiatives taking place within the communications sector. Cable companies participate in a number of working groups that have produced standards and best practices that have aided in the development of effective internal cybersecurity policies and procedures. NIST should focus on identifying and disseminating effective cybersecurity practices already developed through existing sector coordinating councils or other recognized industry standards-setting bodies. The Framework should strive to build upon these existing efforts to the maximum extent possible, by empowering other industries to participate in sector-specific working groups that focus on technical and security issues related to cyber. NIST should identify key industry working groups in each of the critical infrastructure sectors and, where necessary, facilitate the creation of new working groups in individual critical infrastructure sectors if none currently exist. Each of the sector specific agencies should have a facilitating role in consensus building discussions among the private sector.

[25] *ICS-CERT Monitor* at 6.

Most importantly, the Cybersecurity Framework should aim to foster a solutions-oriented, engineer-driven process that encourages experimentation, innovation, and collaboration, while avoiding a top-down approach that shifts the focus to compliance with a set of prescriptive measures. The cyber threat landscape is dynamic and constantly evolving. Government restraint is therefore particularly critical to ensuring that companies can develop appropriate cyber defenses and respond both quickly and effectively to threats. Sectors with a demonstrated commitment to cybersecurity should not have to divert capital and resources away from ongoing efforts to different practices and protocols that may not be as effective in addressing an industry's specialized needs.

To the extent that there are gaps that may not be addressed by current industry practices, those gaps should be filled in the first instance by giving industry the opportunity to develop responses. The existing Sector Coordinating Councils offer an available forum for addressing gaps in industry best practices. NIST should not assume that gaps that it may identify as it develops the Framework must be filled by government-imposed standards or practices. The cross-function internal processes independently developed by the cable industry provide an excellent example of the type of effective institutional innovation that can be adopted and implemented across sectors in the absence of regulatory interference. In creating centralized cybersecurity committees to examine information security and vulnerabilities, cable companies have demonstrated that existing gaps in risk management standards can be effectively addressed by organic "bottom-up" solutions and innovations within the private sector.

CONCLUSION

An effective Cybersecurity Framework will embody existing industry-developed cyber protocols and practices, and avoid forcing businesses to conform to a new set of prescriptive measures. It should offer a broad menu of recommended options and suggested practices that are outcome-oriented, and flexible enough for companies to adapt and customize recommendations to reflect their specific network architecture, business model, and cybersecurity protocols and processes. It should recognize the efforts of sectors such as communications that have devoted considerable resources and efforts to enhancing their cybersecurity. The Framework also should allow for continued innovation and adaptation to reflect the constantly-changing threat landscape.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
Stephanie L. Podey
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

Howard J. Symons
Christopher J. Harvie
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo
701 Pennsylvania Avenue, NW
Washington, DC 20004

April 8, 2013