FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

January 18, 2017

The Honorable Mark Warner
United States Senate
475 Russell Senate Office Building
Washington, D.C. 20510

Dear Senator Warner:

The attached white paper entitled "Cybersecurity Risk Reduction" was prepared by the Chief of the Commission's Public Safety and Homeland Security Bureau. This whitepaper outlines risk reduction activity engaged in by the Commission during my tenure and suggests actions that would continue to affirmatively reduce cyber risk in a manner that benefits from and incents further competition, protects consumers, and addresses significant national security vulnerabilities. Given your leadership on this issue, I thought you would find this white paper of interest.

Sincerely,

Tom Wheeler

Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

# FCC White Paper

---

# Cybersecurity Risk Reduction

**Public Safety & Homeland Security Bureau**
**Federal Communications Commission**
**David Simpson, Rear Admiral (ret.) USN**
**Bureau Chief**

## January 18, 2017

---

# Table of Contents

# Table of Figures

# Introduction

Cybersecurity is a top priority for the Commission. The rapid growth of network-connected consumer devices creates particular cybersecurity challenges. The Commission's oversight of our country's privately owned and managed communications networks is an important component of the larger effort to protect critical communications infrastructure and the American public from malicious cyber actors. The Commission is uniquely situated to comprehensively address this issue given its authority over the use of radio spectrum as well as the connections to, and interconnections between, commercial networks, which touch virtually every aspect of our economy. Other agencies have also begun looking at network-connected devices and the security implications they bring in certain industry segments.[1]

The Commission's rules include obligations for Internet Service Providers (ISPs) to take measures to protect their networks from harmful interconnected devices. These rules make clear that providers not only have the latitude to take actions to protect consumers from harm, but have the responsibility to do so. Reasonable network management must include practices to ensure network security and integrity, including by "addressing traffic harmful to the network," such as denial of service attacks.[2] The Public Safety and Homeland Security's (PSHSB or Bureau) cybersecurity initiatives build upon FCC rules that have, for decades, effectively evolved to balance security, privacy, and innovation within the telecommunications market. The U.S. telecommunications market leads the world as a consequence of this light touch, but surgical, approach.

Commission staff actively work with stakeholders to address cyber challenges presented by today's end-to-end Internet environment. This environment is vastly different and more challenging than the legacy telecommunications security environment that preceded it. Today insecure devices, connected through wireless networks, have shut down service to millions of

---

[1] For example, the U.S. Food and Drug Administration released draft guidance outlining the agency's expectations for monitoring, identifying and addressing cvbersecurity vulnerabilities in medical devices once they have entered the market. *See* U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (2016), at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. http://fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf The U.S. Department of Transportation has proposed guidance on improving motor vehicle cybersecurity. *See* U.S. Department of Transportation. Cybersecurity Best Practices for Modern Vehicles (2016), at http://wwwnhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicales.pdf

[2] *See Protecting and Promoting the Open Internet.* Report and Order, Declaratory Ruling, and Order, 30 FCC Rcd 5601. 5701. para. 220 (2015), *aff'd, United States Telecom v. FCC.* 825 F.3d 674 (D.C. Cir. 2016).

customers by attacking critical control utilities neither licensed nor directly regulated by the Commission. These attacks highlight that security vulnerabilities inherent in devices attached to networks now can have large-scale impacts.

As the end-to-end Internet user experience continues to expand and diversify, the Commission's ability to reduce cyber risk for individuals and businesses will continue to be taxed. But shifting this risk oversight responsibility to a non-regulatory body would not be good policy. It would be resource intensive and ultimately drive dramatic federal costs and still most certainly fail to address the risk for over 30,000 communications service providers and their vendor base.

The Commission must address these cyber challenges to protect consumers using telecommunications networks. Cyber risk crosses corporate and national boundaries, making it imperative that private sector leadership in the communications sector step up its responsibility and accountability for cyber risk reduction. In this vein, the Commission has worked closely with its Federal Advisory Committees (FAC), as well as with its federal partners and other stakeholders, to foster standards and best practices for cyber risk reduction.[3] The Commission worked with the other regulatory agencies to create a forum whereby agency principals share best regulatory practices and coordinate our approaches for reducing cybersecurity risk. A rich body of recommendations, including voluntary best practices, is the result. Industry implementation of these practices must be part of any effort to reduce cybersecurity risk.

The Commission, however cannot rely solely on organic market incentives to reduce cyber risk in the communications sector. As private actors, ISPs operate in economic environments that pressure against investments that do not directly contribute to profit. Protective actions taken by one ISP can be undermined by the failure of other ISPs to take similar actions. This weakens the incentive of all ISPs to invest in such protections. Cyber-accountability therefore requires a combination of market-based incentives and appropriate regulatory oversight where the market does not, or cannot, do the job effectively.

PSHSB has developed a portfolio of programs to address cybersecurity risk in the telecommunications sector in a responsible manner. These initiatives include collaborative efforts with key Internet stakeholder groups; increased interagency cooperation; and regulatory solutions to address residual risks that are unlikely to be addressed by market forces alone.

---

[3] For example, our Technological Advisory Council (TAC) has been examining how to incorporate "security by design" principles into the very fabric of emerging 5G networks, and our Communications Security, Reliability, and Interoperability Council (CSRIC) has been working on cybersecurity in connection with a number of issues, such as improving supply chain risk management, addressing risks associated with legacy protocols such as SS7, and promoting security in networks and devices utilizing Wi-Fi technology. In addition, we have been preparing to launch voluntary, face-to-face engagements, consistent with NIST Framework and CSRIC recommendations, in which providers will collaborate with the Commission to address cyber risk issues in their networks and service environments.

This white paper describes the risk reduction portfolio of the current Commission and suggests actions that would continue to affirmatively reduce cyber risk in a manner that incents competition, protects consumers, and reduces significant national security risks.

## Background

The reduction of cybersecurity risk is a national imperative that includes safeguarding our communications networks themselves. Businesses and consumers rely on our wired and wireless broadband networks every day. If these networks are embedded with vulnerabilities, it puts everyone who uses them at risk. The Internet is a network of networks – risk in one network can propagate to others, imposing hidden risk throughout our connected economy and society.

Reducing risk in our communications networks is complicated by unique economic factors. The overwhelming majority of our broadband infrastructure is owned and operated by commercial entities. ISPs, like all modern businesses, have economic incentives that drive investment decisions. When deciding how much to invest to reduce cyber risk, the cost-benefit analysis of ISPs naturally considers the risks to the firm. Unfortunately, relying on market forces alone fails to adequately weigh the risks imposed on third parties who rely on the networks and services they provision. A cybersecurity gap confronts the public. With the ISPs facing limited competition and low return on cyber investment, this is a gap that the free market is unlikely to fill.

With a Congressional mandate to assure the safety and resiliency of our nation's communications networks, the Federal Communications Commission (FCC or Commission) has a clear role and responsibility in addressing residual cybersecurity risk – *i.e.*, the risk remaining after market participants have acted to remediate cyber risk that directly affects their business interest. Residual risk can be large and is ultimately imposed on stakeholders that have scant awareness of its presence or means to remediate it. The Commission is uniquely situated to address this issue given its authority over the use of radio spectrum as well as the connections to and interconnections between commercial networks, which touch virtually every aspect of our economy.[4] The Commission has a proven track record of working with commercial carriers to fortify our networks and mitigate vulnerabilities, including cyber threats like Denial of Service (DoS) attacks, IP-route hijacking and address spoofing. In addition, we have also had effective engagements with the security agencies, which have informed our technical assessments and appreciation of the challenge. Similarly, our collaboration with other regulators through the Cybersecurity Forum for Independent and Executive Branch Regulators has informed our economic analysis and appreciation of the unaddressed residual risk.

[4] *See* Appendix A, prepared in coordination with the Office of General Counsel and Office of Engineering and Technology, for a summary of the FCC's cybersecurity authorities, including those most relevant to securing the Internet of Things.

As cybersecurity challenges grew in scale and significance over the past decade, it became clear that a new approach was warranted. In recent years, the Commission has advanced a new paradigm for cybersecurity that acknowledges prescriptive regulations could never hope to keep pace with such a fast-changing issue. Our strategy relies on voluntary efforts by ISPs within mutually agreed parameters, combined with regulatory oversight and an increased emphasis on accountability to assure companies are mitigating their cyber risk. Key Commission actions include:

- *Promoting best practices*. Working with industry and external partners to develop a harmonized, rich repository of standards and best practices for cyber risk management.
- *Making cybersecurity a forethought not an afterthought.* Promoting security by design efforts to incorporate cyber during the development phase of new products and services and adopting rules requiring licensees for 5G wireless networks to submit a cybersecurity plan before commencing operations.
- *Increasing situational awareness*. Strengthening our network outage and data breach reporting requirements.
- *Improving information sharing*. Adopting real-time cyber threat information sharing with federal partners and promoting sharing among private carriers.
- *Establishing cybersecurity as integral to the Public Interest*. Identifying cybersecurity as a consideration of merger reviews.

This paper lays out these and other activities in greater detail. More importantly, it looks ahead and highlights emerging cybersecurity issues that will demand the FCC's attention and offers potential solutions.

For example, the Internet of Things (IoT) promises 200 billion connected objects by the year 2020. This exponential growth in potential attack vectors will require diligence and fresh thinking on the part of network operators and the FCC.

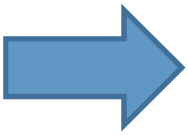
The unique vulnerability of small and medium carriers is another area in need of the Commission's attention. Their relative lack of resources to invest in cybersecurity may make them targets of attack. This paper explores new ideas for using federal funding to establish a baseline level of cybersecurity across all telecommunications providers.

# Lines of Effort

Cyber risk management is applied in multiple dimensions within the communications sector. First and foremost, cyber vulnerabilities, when exploited, negatively impact availability through disruptions to consumers and communities. Communications cyber vulnerabilities, when exploited, can also result in impaired integrity. Integrity can be lost when communications are diverted in ways that are not apparent to users or when modified or malicious communication is

injected that users wrongly trust, or any number of privacy exploits. Communications with weak or nonexistent encryption can result in loss of confidentiality that, while not immediately apparent to users, are nonetheless harmful to privacy and can result in a range of potential negative consumer impacts.

Elements of cyber risk appear in virtually all applications of communications with different consequences. Exploits of routine communications are far less consequential than similar exploits on public safety communications, for example. The Commission has applied a holistic approach to mitigating cyber risk that spans applications, using a light regulatory touch that looks first to industry leadership (see text box below). It participated in deployment of and continues to structurally align Commission cybersecurity around the *2014 National Institute of Standards Cybersecurity Framework* (*2014 NIST Framework*) which is discussed more fully below.[5]



The FCC's cyber risk reduction has several lines of effort to address the multi-dimensional aspect of risk reduction in the communications sector, as discussed in greater detail below.

## The FCC's "New Paradigm"

In 2014, the Commission embarked upon a new paradigm for how the FCC would address cybersecurity for our nation's communications networks and services. It looks first to private sector leadership, recognizing how easily cyber threats cross corporate and national boundaries. Where market incentives cannot fully address cyber risk, however, the FCC has stood ready to take action. In this manner, the FCC has carefully balanced a market-based approach with appropriate regulatory oversight where the market is inadequate to address cyber risks fully.

Problems known as "market failures" can discourage investment and contribute to the insecurity of the critical communications network. (A thorough discussion and graphical analysis of market failure can be found in Appendix B, *PSHSB Cybersecurity Program and the Market for Cybersecurity in the Telecommunications Sector,* Staff Report, December, 2016.) Widespread threats and falling consumer confidence in the Internet indicate that there is a high probability of market failure due to inadequate competition, lack of direct return on investment, and a lack of information. Why do firms invest less than would be best for society as a whole? Fundamental economic theory explains why markets – the driving force in our economy – can sometimes fail to produce the best outcomes. Classic market failures include externalities, market power, and information problems.

**Externalities** are impacts on third parties. When companies invest in cybersecurity, they do not

[5] *Framework for Improving Critical Infrastructure Cybersecurity,* National Institute for Standards and Technology (Feb. 12, 2014).

fully consider the impact of those investments on other companies and consumers. For example, an ISP's decision to invest in cybersecurity protection provides a safer environment not only for the ISP, but for everyone on the network. If it considered the total benefit of its investment, it would invest more. But it does not, because the return on that investment is received by others.

**Market power** exists when a provider has no (or few) competitors. If consumers have few competitive ISP choices, they may not be able to select an ISP based on cybersecurity practices.

**Information problems** can impede investment in cybersecurity because it may be difficult to determine the veracity of supplier or ISP claims of cybersecurity practices. ISPs cannot individually overcome these market-wide barriers to stronger security. Broader action may be called for – by voluntary industry associations and/or by government action. Where there is clear evidence of market failure, the FCC may have reason to take stronger measures to motivate market participants to improve cybersecurity preparedness in the communications sector.

Because of market failure, market forces alone do not provide necessary cybersecurity investment for society as a whole. The FCC has tools to tip the commercial balance toward more investment in cybersecurity in a manner that better meets society's needs as a whole. Some of the tools the Commission can leverage are discussed below.

*Figure 1 - The FCC's "New Paradigm"*

### *Standards and Best Practices*

The Commission does not automatically presume that market failure is inhibiting private sector investment. Some of the greatest reductions in risk are achieved by aligning best practices with natural market incentives. The Commission often asks its private/public partnerships, such as FACs, to provide recommendations for our use in addressing cyber risk management in the sector. FACs are subject to the Federal Advisory Committee Act[6] and provide the Commission with independent advice on topics of the Commission's choosing. They include diverse voices from across the spectrum of communications sector stakeholders. The Commission frequently uses recommendations from these groups to guide policy decisions on cyber risk management. Often the Commission's convening authority is enough to bring an issue or vulnerability to the attention of the right stakeholders, with providers then addressing the issue effectively and visibly without further FCC engagement required.

When emerging technologies enter the picture, the Commission frequently begins its work with one such FAC, the Technological Advisory Council (TAC). The TAC provides the Commission with recommendations on technologies that are on the cusp of network deployment and, in the case of cybersecurity, helps to "bake" security into the design phase. The TAC's focus now is on 5G security, where its work will help to ensure that early 5G standards will incorporate security elements. For example, the TAC has made significant recommendations on

[6] 5 U.S.C. App. 2.

groundbreaking technologies like IoT,[7] Software Defined Networks (SDN),[8] and Software Defined Radio (SDR).[9]

This engagement has and should continue to benefit from the public articulation of security objectives, the work of industry, standards bodies and academia to incorporate cyber security as a design factor in their new products and services and most importantly, the transparent communication of the evolving plans in "plain speak" so that public comment can highlight areas where societal security expectations are not being addressed.

## The Internet of Things (IoT)

The burgeoning – and insecure – IoT market exacerbates cybersecurity investment shortfalls that are highlighted above. Because of negative externalities (third parties affected by insecure IoT), the private sector may not have sufficient incentives to invest in cybersecurity beyond their own corporate interests. (Bruce Schneier, *Security Economics of the Internet of Things*, Schneier on Security (2016), at www.schneier.com/blog/archives/2016/10/security_econom_1.html.) The attack surface offered by the IoT is growing rapidly. (Steve Morgan, *Top 5 Cybersecurity Facts, Figures and Statistics for 2017*, CSO (2016).) The large and diverse number of IoT vendors -- who are driven by competition to keep prices low - hinders coordinated efforts to build security by design into the IoT on a voluntary basis. Left unchecked, the growing IoT widens the gap between the ideal investment from the commercial point of view and from society's view. This gap reflects risks on many sectors as the IoT expands in public safety communications, industrial control systems and supervisory control and data acquisition (SCADA), the use of machine-to-machine sensors, smart city technology, and broadband-dependent critical infrastructure.

In November 2016, the Broadband Internet Technical Advisory Group (BITAG) produced a report that recommends steps to address key security concerns brought by the IoT. (*See* www.bitag.org/report-internet-of-things-security-privacy-recommendations.php.) Also in 2016, the Department of Homeland Security issued strategic principles for securing the IoT and called on the public and private sectors to work together to improve IoT security. (*See* www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL.pdf.)

The Bureau has recently issued a Notice of Inquiry (NOI) to develop a record and identify residual risk in the IoT commons. (*See Fifth Generation Wireless Network and Device Security,*

[7] *See* 5G Cybersecurity Subcommittee, at https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/TAC-5G-Cybersecurity-Subcommittee-09-12-16.pdf.

[8] *See* Securing SDN NFV Sub-Working Group, at *h*ttps://www.fcc.gov/oet/tac/tacdocs/reports/2016/2016-FCC-TAC-Securing-SDN-NFV-White-Paper-v1.0.pdf.

[9] *See* Software Configurable Radios Subcommittee, at http://www.fcc.gov/oet/tac/tacdocs/reports/2016/FCC-TAC-CS-SCR-White-Paper-20161202.pdf.

*Notice of Inquiry*, PS Docket No. 16-353, DA 16-1282 (rel. Dec. 16, 2016), at http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1216/DA-16-1282A1.pdf.) In addition, building on the work of the TAC described below, the Bureau recommends the following options, depending on the extent to which elements of market failure risks are found to be acting to inhibit market-based solutions:

- Charge CSRIC to recommend cyber risk reduction standards and best practices, including application of the Botnet Code of Conduct previously recommended by CSRIC, to IoT endpoints.
- Charge CSRIC to recommend roles for members of the 5G ecosystem to mitigate cyber risks to the emerging 5G network infrastructure.
- As the current Chair of the Cybersecurity Forum for Independent and Executive Branch Regulators, convene a task force to assess the full scope of IoT cyber risk to critical infrastructure, existing authorities requiring statutory change.
- Drawing upon these and other multi-stakeholder engagements, issue a Notice of Proposed Rulemaking (NPRM) proposing regulatory measures to help address residual cyber risks that cannot be addressed through voluntary measures alone. The NPRM could propose, for example, changes to the FCC's equipment certification process to protect networks from IoT device security risks.

Appendix A, prepared in coordination with the Office of General Counsel and Office of Engineering and Technology, summarizes the FCC's cybersecurity authorities, including those most relevant to securing the IoT.

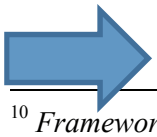
*Figure 2 - The Internet of Things*

When these emerging technologies reach a certain level of maturity, their work is passed to another FAC, the Communications Security, Reliability and Interoperability Council (CSRIC), which recommends best operational practices and procedures for technologies in deployment. The members of the TAC, most recently recommended formalizing a process in which early design work in the TAC can be handed off routinely to CSRIC to support implementation when the time is right. This process will be inaugurated in CSRIC VI with IoT, 5G, and SDN as the subject technologies.

CSRIC, like the TAC, is a FAC that develops recommendations for the telecommunications sector based on specific requests from the Commission. CSRIC emphasizes implementation aspects of communications technologies that are in use today. Over the years, CSRIC has recommended expert-based best practices that communications providers use at their discretion to promote communications security and reliability, including cyber risk management in Wi-Fi networks and legacy protocols, like Signaling System 7 (SS7), that are approaching end-of-life and are less attractive targets of investment.

In 2013, NIST used a multi-stakeholder process to develop the business-driven, proactive Framework (the *2014 NIST Framework*) to promote voluntary cyber risk management in critical infrastructure sectors.[10] The *2014 NIST Framework's* processes and practices, with their emphasis on governance, are tools to manage cyber risk holistically in companies of all sizes and sectors of the economy. The Commission charged CSRIC to apply the *2014 NIST Framework* to the communications sector by recommending a new flexible, voluntary approach that would reduce cybersecurity risk in the sector and provide assurances to the Commission and the public that communications providers are implementing needed cyber risk management processes and practices. In response, CSRIC has recommended a comprehensive approach to cyber risk management in the communications sector based on the *2014 NIST Framework*. Among these, "CSRIC recommend[ed] that the FCC, in partnership with DHS, participate in periodic meetings with communications sector members, in accordance with PCII protections,[11] to discuss their cybersecurity risk management processes and their use of the NIST Cybersecurity Framework or equivalent construct."[12] The Bureau routinely works with companies and their associations to discuss cyber security risk factors and risk reduction best practices. The Bureau believes these meetings would be further enhanced by a formal commitment towards protected handling of sensitive company information.

CSRIC supports the Commission's continuing work to better understand and address a wide range of technology risk, over-reliance on GPS for network timing is but one example. CSRIC evaluated other Global Navigation Satellite Systems and terrestrial systems for Position, Navigation, and Timing (PNT), identifying alternate sources of network timing to help mitigate some of this risk. Follow on work will identify best practice implementation and any remaining barriers to this critical element of critical infrastructure robustness.



[10] *Framework for Improving Critical Infrastructure Cybersecurity,* National Institute for Standards and Technology (Feb. 12, 2014).

[11] Congress created the Protected Critical Infrastructure Information (PCII) Program under the Critical Infrastructure Information (CII) Act of 2002 to protect private sector infrastructure information voluntarily shared with the government for the purposes of homeland security. The Final Rule at 6 C.F.R. Part 29, published in the Federal Register on September 1, 2006, established uniform procedures on the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security. The protections offered by the PCII Program enhance the voluntary sharing of critical infrastructure information between infrastructure owners and operators and the government, and give homeland security partners confidence that sharing their information with the government will not expose sensitive or proprietary data.

[12] *See* Cybersecurity Risk Management and Best Practices, Final Report, March 2015 https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

The Commission should consider adopting the Declaratory Ruling on circulation which would implement CSRIC's recommendations with respect to confidential, company-specific meetings (engagements) and appropriately shield them from the Commission's enforcement and regulatory processes. Separately, the Commission should consider re-chartering CSRIC for its sixth two-year term. CSRIC VI will be tasked with developing standards and best practices on 5G, IoT, public safety and emergency response, legacy protocol cyber risk reduction, WiFi security, software defined network security, and priority services.

### *Situational Awareness*

The Commission's mission to ensure that the United States has reliable communications requires that it obtain information about communications disruptions and their causes, both to prevent future disruptions that could occur from similar causes, and to enable the use of alternative communications networks while the disrupted facilities are being restored.[13] A key role of the federal government is to understand residual cyber risk and manage this risk appropriately within our plenary area of responsibility. As a practical matter, in order to help implement this role, the FCC must have a repository of data documenting when communications failures occur. To do this, the Commission, pursuant to Part 4 of the our rules,[14] requires communications providers to file reports in the Network Outage Reporting System (NORS), providing information about an outage, including the suspected cause and steps taken to remediate the outage and restore service.[15] The data generated by these requirements are used by the National Cybersecurity and Communications Integration Center (NCCIC)[16] to support situational awareness and by Commission staff to identify areas where communications reliability suffers, thereby guiding remediation actions led by the Bureau, virtually all of which are developed in collaboration with providers. When carriers are aware of a malicious cause of an outage, which could be the result of a cyber incident, they are required to provide that information as part of their report. In this way, the FCC currently obtains information, albeit limited, on cyber causes of outages.

In May 2016, the Commission proposed extending the Part 4 Outage Reporting rules in several ways: the Commission proposed requiring carriers to report on "unintended changes to software or firmware or intended modifications to a database,"[17] and further proposed that such events be

---

[13] *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16836-37, para. 11 (2004).

[14] 47 CFR § 4 *et seq*.

[15] *See* 47 CFR § 4.11; *see also* FCC, *Network Outage Reporting System (NORS)* (Jul. 21, 2016), at https://www.fcc.gov/network-outage-reporting-system-nors. *See* links to "NORS Quick Start Guide" and "NORS User Manual."

[16] *See* https://www.us-cert.gov/nccic

[17] *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report

reportable even if they do not rise to the level of an "outage" as defined in the part 4 rules.[18] In the future, the Commission should consider adopting these proposals, to enable it to obtain timely information on major cyber incidents, to improve its situational awareness and enable it to coordinate and facilitate cyber-incident response.

Further, while the Commission has adopted outage reporting requirements for communications platforms such as wireline, wireless, satellite, interconnected VoIP, and, most recently, submarine cables, the Commission has recently sought comment on extending reporting to outages affecting broadband services. The Commission needs to be kept aware of the status of communications network and service reliability. First and foremost, this information provides a significant national and public safety benefit.[19] Yet information obtained from providers about disruptions to communications is not keeping pace with the introduction of new technologies. For instance, reporting requirements for newer technologies, such as broadband and Internet Access, are not clear.[20] The Commission has proposed updates to its Part 4 rules to keep pace as commercial communications transition to broadband technologies.[21] Accordingly, the Commission, in 2016, issued a Further Notice of Proposed Rulemaking (FNPRM) proposing updates to our outage reporting rules. The proposed rules would require communications providers to file in instances where the Broadband Internet Access Service (BIAS) is effectively "down."[22] (Packets may still be delivered but normal customer functions are not being supported.) In addition, carriers would be required to indicate, in their outage reports, whether the outage has a cyber or otherwise malicious cause.

---

and Order, Further Notice of Proposed Rulemaking, and Order on Reconsideration, 31 FCC Rcd 5817, 5868, para. 122 (2016).

[18] *Id.* at 5869, para. 125.

[19] *See New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, (2004) (2004 Part 4 Order).

[20] *Id*.

[21] *See* 2016 Part 4 FNPRM, FCC 16-63. The 2016 Part 4 FNPRM was published in the Federal Register on July 12, 2016. 81 Fed. Reg. 45095 (Jul. 12, 2016).

[22] The Part 4 FNPRM proposed to apply the definition of "Broadband Internet Access Services" or "BIAS" that was in the 2015 Open Internet Order. In that proceeding, the Commission defined BIAS to mean "[a] mass market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part." 47 CFR § 8.2(a). *See also* 2015 Open Internet Order, 30 FCC Rcd at 5682-86, paras. 187-93.

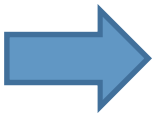
## Submarine Cables

Submarine cables traversing the Atlantic and Pacific Oceans carry the vast majority of international internet traffic, and are vitally important to our nation's economy and national security. Due to this importance, the Commission has adopted an outage reporting requirement for submarine cables licensees. (*See Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Data*, GN Docket 15-206, Report and Order, 31 FCC Rcd 7947, 7948 para. 1 (2016)) This reporting requirement will gather critical data about the submarine cable sector, and will include those outages caused by cyber incidents. Through this requirement, the Commission will gain a more comprehensive picture of the entire threat landscape facing our nation's critical infrastructure.

*Figure 3 - Submarine Cables*

In 2016, the Commission adopted rules implementing the Communications Act's (47 USC 222's) privacy requirements for broadband ISPs. As part of this proceeding, the Commission adopted common-sense data breach notification and data security requirements. Once these rules become effective, providers who suffer a data breach must notify the Commission of the breach. Breach notifications will empower customers to protect themselves against further harms, help the Commission identify and confront systemic network vulnerabilities, and assist law enforcement agencies with criminal investigations. The Bureau is tasked with developing, implementing, and maintaining the data breach reporting portal. Providers and telecommunications carriers must also take reasonable measures to secure customer proprietary information from unauthorized use, disclosure, or access. A provider that fails to secure customer information cannot protect its customer from identity theft or other harms, nor can it assure its customers that their choices regarding use and disclosure of their personal information will be honored. To comply with the data security requirement, providers must adopt security practices appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility. This standard underscores the importance of robust data security standards, while providing flexibility for the standard to change as technology and best practices evolve over time.

To further facilitate rapid assessment and appreciation of cyber incidents and facilitate response actions, the FCC Operations Center (FCCOC) stays in constant contact with the NCCIC, the National Military Command Center, the National Infrastructure Coordinating Center, the intelligence community, and other key cyber awareness and response entities within the federal government. The FCCOC operates 24/7/365, leveraging various redundant facilities and communications systems across all levels of classification. As part of the broader interagency effort to prepare for significant cyber incident response, the Commission also engages regularly with more policy-focused response entities such as the National Security Council-led Cyber Response Group and Domestic Resilience Group.



The Commission should consider expanding its outage reporting rules to require carriers to report on cyber events, irrespective of whether they cause a disruption to communications. For example, a route hijack may not result in a disruption to communications from the customer's point of view, but it may expose their communication to unintended inspection or corruption by third parties. In addition, given our increasing reliance on IP-based communications, including support of essential public safety communications, the Commission should consider expanding its outage reporting rules to include IP-based communications generally. Through reports of data breaches, and working with communications providers, the Bureau will be able to analyze breach trends and identify systemic vulnerabilities, and through industry outreach, work collaboratively with providers to improve data security.

### *Security by Design*

As equipment suppliers and communications providers rush to satisfy market demands, security has often taken a backseat to swift development and introduction of new features. This results in the rollout of new products that lack important security protections, which may (or may not) be fixed after they reach the market, in a practice known as "after-market patching." Security by design is a development practice that reduces cyber risk by using a disciplined process of continuous testing, authentication safeguards and adherence to best development practices. An emphasis on building security into products counters the all-too-common tendency for security to be an afterthought in development. The Bureau believes that this approach will diminish the need for after-market patching.[23]

Security by design principles "embed security in the technology and system development from the early stages of conceptualization and design."[24] Software developers, including the open source community, and device manufacturers can build security into new products and services by including it in the environments they use to manage the development process explicitly. Security standards should be used to guide the development process and final design reviews should include security requirements so that no produce or service can leave the development environment without satisfying basic security elements.

**5G Security**

The next evolutionary step in wireless broadband communication, 5G, is expected to support a highly diverse range of new applications, user requirements, and connected

[23] *See* https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

[24] European Security Research and Innovation Forum, 2009, at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.

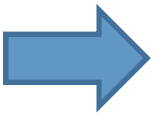
devices, including smartphones, sensors, robotics, mission-critical wireless communication, and automated guided vehicle systems for the automotive and automotive supply industries. As described above in the Standards and Best Practices section, 5G networks will be subject to many of the cyber risks associated with the IoT. Furthermore, 5G will enable a massive expansion of IoT endpoints that lack the processing power and memory needed for robust security protections. Fortunately, 5G is at an early phase in its development and, if security is designed in, it may be able to mitigate the cyber risk from these IoT endpoints. The Commission is moving to take advantage of 5G's pre-deployment status in the following ways:

1. The TAC, in coordination with the Alliance for Telecommunications Industry Solutions (ATIS), has recommended contributions to the 3rd Generation Partnership Project (3GPP), a group of standards development organizations that work together to produce reports and specifications that define 3GPP technologies. By working with standards bodies so early in the development life cycle, the objective of security by design for 5G should be achievable. ATIS has adopted TAC recommendations, which will be submitted to 3GPP as a Change Request (CR) to 3GPP as needed. ATIS is expected to submit the first CR to 3GPP in February 2017. (*See* https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/TAC-5G-Cybersecurity-Subcommittee-09-12-16.pdf)
2. In its July 2016 *Spectrum Frontiers Report and Order*, the Commission adopted a rule requiring Upper Microwave Flexible Use Service licensees to submit general statements of their network security plans prior to commencing operations. The statements are designed to encourage licensees to build security into their new 5G networks. The statements will also facilitate the Commission's ability to help identify security risks, including areas where more attention to security may be needed, and in disseminating information about successful practices for addressing risk. (*See* http://www.fcc.gov/document/spectrum-frontiers-ro-and-fnprm)
3. As discussed above, the Bureau has released an NOI intended to promote security by design for 5G devices, equipment, network planners, and designers through targeted inquiry on standards-driven planning by communication service providers and manufacturers. The 5G NOI solicits public comment regarding the opportunity to employ security by design as a core principle from the beginning of 5G development.
4. The Bureau also recommends considering convening workshops to promote a dialog on challenges, successes, and related issues associated with the 5G security by design goal.

*Figure 4 - 5G Security*

In March 2016, CSRIC provided the Commission with recommended best practices to enhance the security of the hardware and software in the core communications network. CSRIC then examined frameworks commonly used for self-assessment of these best practices, including NIST Special Publications (SP) and International Organization for Standardization/International

Electrotechnical Commission (ISO/IEC) 27000 standards. In September 2016, CSRIC recommended that communications network organizations provide assurances to the FCC of their use of security-by-design best practices. These assurances would be provided during the voluntary cyber assurance meetings with the FCC described above. These meetings provide an opportunity for participating companies to share information regarding cyber policies, threats, or attacks. The in-person cyber risk management meetings would be the best venues for companies to describe their security practices candidly.[25]



The Commission should consider further promotion of "security by design" and encourage communications and equipment providers to build security into their development process. For several database intensive telecommunications control functions, the Commission has further incentivized early consideration of security by design by requiring submission of a cybersecurity plan with implementation of the new services – Number Portability, 911 Location Accuracy, 3.5 GHz Shared Spectrum Access, and 5G Upperbands are good examples of this.

### *Targeted Risk Reduction for Small and Medium Providers*

In March 2015, CSRIC IV recommended the Commission adopt voluntary mechanisms to implement cyber risk management practices based on application of the *2014 NIST Framework* to the communications sector.[26] The CSRIC effort included a Small and Medium Business Group specifically focused on how to apply the *2014 NIST Framework* to small and medium sized operations, while respecting challenges related to their size and limited resources.

The FCC understands that smaller carriers often have fewer resources available to them, and Section 9.9 of the CSRIC Report offers guidance designed specifically for smaller carriers (see text box below). This section provides smaller carriers with a formalized and structured risk-management approach to address cybersecurity, applying the *2014 NIST Framework* based upon their unique needs and operational environment.

The Commission has included cyber risk reduction as a cost element for subsidies to small and medium providers. For example, in July 2014 the FCC adopted the *Rural Broadband Experiments Order* as part of the Connect America Fund (CAF), the portion of the Universal Service Fund (USF) that goes towards supporting communications infrastructure in rural and

[25] *See* discussion on page 7 above under "Standards and Best Practices".

[26] *See* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

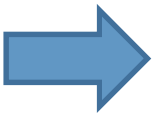
high-cost areas.[27] As a new part of the CAF, the FCC allocated $100M for funding experiments whereby providers bid in a reverse auction to bring voice and broadband-capable networks to residential and small business locations in rural communities. In its Order establishing selection criteria for the Rural Broadband Experiments, the Commission observed that "[f]or broadband networks across the nation to be considered advanced, robust, and scalable, they must also be secure and resilient in the face of rapidly evolving cybersecurity threats."[28] The Commission further noted that "[s]mall providers in diverse service areas play a key role because any point of weakness in today's interconnected broadband ecosystem may introduce risk into the entire network of interconnected service providers."[29] Small companies should avail themselves of Commission-provided training resources and guidance.[30] This support includes technical expertise, training resources, cyber risk management program development and internal policy guidance.

## Challenges for Small Service Providers

Smaller communications providers are just as vulnerable as large providers and face unique challenges related to size, including limited access to financial, staff and technical resources. Further, their relative lack of resources to invest in cybersecurity may make them targets, whether for direct exploitation or as a means to access more high-profile targets. For example, in its June 2016 Information Sharing Barriers Report, CSRIC found that small and medium network service providers face disproportionate barriers to information sharing, particularly with respect to financial considerations. Accordingly, the Bureau recommends establishing a funded Information Sharing and Analysis Organization (ISAO) Pilot Project consisting of ten to twenty smaller communications providers. The pilot would take advantage of conclusions from a similar program funded by CTIA and other associations. The pilot would develop an information sharing platform relying on an automated information system that would enable small carriers to participate and choose the level of information they want to receive. Removing the burden of independently resourcing costs for cybersecurity M2M information sharing and analysis should help protect and enhance credible competition while addressing cyber threats collectively in a manner that would be more efficient than adding to subsidies for each of the over 1200 small broadband service providers.

*Figure 5 - Challenges for Small Service Providers*

[27] *Connect America Fund; ETC Annual Reports and Certifications*, WC Docket Nos. 10-90, 14-58, Report and Order and Further Notice of Proposed Rulemaking, FCC 14-98 (2014).
[28] *See Technology Transitions,* GN Docket Nos. 13-5 and 13-353, WC Docket No. 10-90 and 13-97, CG Docket Nos. 10-51 and 03-123, Order, 29 FCC Rcd 1433 ¶ 49 2014).
[29] *Id.*
[30] *Id.*



The Commission should consider making cyber risk reduction an element in determining subsidies for small and mid-sized communications providers via the USF. The Commission should also consider funding an ISAO Pilot Program to enable small and mid-sized communications providers to gain experience and benefit from real-time cyber threat information sharing.

### *Public Safety*

Next-generation 911 (NG911) systems, which rely on IP-based protocols and services, will allow responders to take advantage of capabilities such as text and video messaging. Public safety answering points (PSAPs) will be able to route calls and provide alternative routing to ensure resiliency during an emergency or disaster. However, in spite of these important benefits, cybersecurity challenges increase when PSAPs are connected to multiple devices and networks that make use of the Internet protocol.

In the FCC's 8th Report to Congress on the collection and use of 911 fees,[31] on the topic of cybersecurity preparedness for PSAPs, 38 states, American Samoa, Puerto Rico, and the US Virgin Islands indicated that they spent no 911 funds in 2015 on 911–related cybersecurity programs for PSAPs. Only nine states and the District of Columbia reported that they had made cybersecurity-related expenditures. More specifically, the report found that ten states reported that one or more of their PSAPs either implemented a cybersecurity program or participated in a regional or state-run cybersecurity program the number of PSAPs in 2015, but 15 states, American Samoa, the District of Columbia, Puerto Rico, and the US Virgin Islands reported that their PSAPs did not implement or participate in cybersecurity programs, and 22 states reported that they lacked data or otherwise did not know whether their PSAPs had implemented or participated in cybersecurity programs. More generally, with respect to whether states and jurisdictions adhere to the *2014 NIST Framework* for networks that support one or more PSAPs, eleven states and the District of Columbia reported that they do adhere to the *2014 NIST Framework*, eight states and Puerto Rico reported that they do not, and 27 states, American Samoa, and the US Virgin Islands indicated they did not know. The shortfall is understandable. Communications providers were responsible for end-to-end security and delivery of 911 voice calls in an earlier Public Switched Telephone Network (PSTN). More modern IP-based 911 service changes service demarcation boundaries and the enhanced processing for call handling, dispatch, and records management has expanded the 911 attack surface. Many jurisdictions have not yet organized their cybersecurity programs.

[31] *See* FCC, Eighth Annual Report to Congress on the Collection and Use of 911 Fees and Charges, Dec. 30, 2016, at 83-89, available at https://www.fcc.gov/general/911-fee-reports.

The Commission formed the Task Force on Optimal PSAP Architecture (TFOPA) to provide recommendations on how to best prepare and defend public safety networks (*e.g.*, FirstNet, ESINets, NG911) from current and emerging cyber threats. TFOPA delivered recommendations on December 2, 2016,[32] which the Bureau is currently reviewing. TFOPA recommended that subsequent work be considered in areas like information sharing, workforce training, and data analytics.

Based on evidence that communications providers were not adopting critical 911 best practices, the Commission, in December 2013, adopted a Report and Order requiring covered 911 service[33] providers to certify compliance with specified best practices or reasonable alternative measures. The Bureau should examine these rules to determine whether or not proposals should be made to expand them in light of looming cyber risks to the 911 system. For example, as the migration NG911 continues apace, PSAPs will be exposed to new types of cyber risk that can cause the same types of catastrophic outages that led to the original 911 certification obligations.

Commercial communication networks are critical to the President's ability to exercise command and control of military forces, perform national outreach to the American people, maintain ties and coordination with allies and international partners, and communicate with Federal, State, and local officials during national security and emergency situations. National Security and Emergency Preparedness (NS/EP) priority communications are intended to provide the President, as well as emergency response officials at all levels of government, with the ability to communicate under all circumstances so that they may carry out critical and time sensitive missions. This is accomplished through priority access to commercial wired and wireless communications systems.

The current generation of NS/EP priority communication programs was designed in a voice-centric, circuit-switched communications environment where circuits were permanently or temporarily dedicated to single customers – an environment very different from today's emerging data-centric, packet-based communications infrastructure / ecosystem that relies on multiple, simultaneous paths of transmission. The digitized and interconnected nature of communications now makes the nation's communications backbone susceptible to new and proliferating global threats and hazards. A focused attack, cyber or physical, on core

[32] https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf

[33] Covered 911 Service Providers are entities that: Provide 911, E911, or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities, directly to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as defined in 47 C.F.R §64.3000(b); or Operate one or more central offices that directly serve a PSAP. A central office directly serves a PSAP if it (1) hosts a selective router or ALI/ANI database, (2) provides equivalent NG911 capabilities, or (3) is the last service-provider facility through which a 911 trunk or 10-digit administrative line passes before connecting to a PSAP.

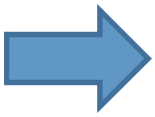
communications infrastructure could prevent the conveyance of the nation's most critical and time sensitive communications. The migration of critical infrastructure Industrial Control System and Supervisory Control and Data Acquisition (ICS and SCADA) functions to commercial IP-transport further exacerbates these security risks, as disasters or attacks that constrain available broadband capacity could block effective control of vital communications infrastructure, when needed most.

Existing NS/EP programs are slowly converting priority services from circuit-switched networks to IP-based networks for voice telephony, but they do not address new priority communications threats and opportunities, including transmission of text, data, and video. The multi-path transmission of IP communications also raises the importance of universal acceptance and handling of priority communications across domestic networks and carriers.

## The Emergency Alerting System (EAS)

As the cyber-attack on French TV Monde and the intentional "Zombie" alert in 2013 attest, broadcast-based networks and the Emergency Alert System (EAS) currently have significant vulnerabilities and are at risk of future compromises. The accidental triggering of a Presidential EAS alert by the Bobby Bones Show in 2014 is further evidence of the vulnerability of the EAS. These vulnerabilities, including the insecure nature of the legacy broadcast format as well as the unfamiliarity of smaller broadcast participants with internet security, need to be addressed to prevent further compromise of the system. In order to ensure the overall integrity of the EAS, the Bureau recommends that the Commission take measures to enable and encourage EAS Participants to improve the security, reliability and accountability for their systems. As noted in the December 2016 Public Notice on the 2016 nationwide EAS test, there is an opportunity and need to strengthen the EAS, since, while generally successful, the test was conducted in an environment that posed a low threat for cyber exploits. (*See Public Safety and Homeland Security Bureau Releases Its Initial Findings Regarding the 2016 Nationwide EAS Test*, PS Docket No. 15-94, Public Notice, DA 16-1452 (PSHSB Dec. 28, 2016) at http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1228/DA-16-1452A1.pdf). Ensuring EAS Participants integrate basic cyber security guidelines into EAS equipment readiness rules assisting them in self-assessment and self-correction of vulnerabilities in their facilities would harden the EAS against the range of cyber exploits generally present for actual alerts and tests.

*Figure 6 - The Emergency Alert System (EAS)*



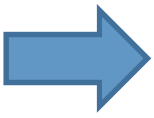
The Commission should consider promoting EAS cyber risk reduction by ensuring that EAS Participants integrate basic cybersecurity guidelines into EAS equipment readiness rules. Furthermore, following the release of recommendations from the NS/EP Executive Committee's working group on

priority services, coupled with the expected delivery of CSRIC V priority services recommendations, the Commission should consider the necessity of appropriate rulemaking efforts to ensure the availability and reliability of NS/EP priority communications in the IP-based environment.

### *National Security*

The last several years have shown that the federal effort to defend the nation from cyber threats must be an "all hands" effort, with defense capabilities, the intelligence community, law enforcement, and critical infrastructure-focused agencies (regulatory and non-regulatory) all playing important roles. FCC engagement with this broader government effort has begun to yield results, and continued engagement will be essential going forward. The FCC has coordinated carefully with partners in law enforcement and the intelligence community to foster a deep dialog regarding emerging risks in communications – both from new technologies and new exploits of legacy technology; associated vulnerabilities in current and future communications systems; adversary tactics, techniques, and procedures to exploit these vulnerabilities; and government and industry actions that may mitigate the overall risk.

This engagement also includes operational coordination such as planning and exercising response capabilities where Commission authorities may be relevant to shape response actions – for example by rapidly providing special temporary authorities (STAs), waivers, or other regulatory actions. Based on the FCC's robust authorities and deepening relationships, the Commission is increasingly integral to cyber response planning and execution, as demonstrated by its inclusion in relevant Presidential Policy Directives and Executive Orders; the National Cyber Incident Response Plan; and plans for use of Presidential authorities during time of war or national emergency. During 2016, the Commission participated in several cyber-related exercises, including Cyber Storm V and Cyber Guard 16. As a result of lessons learned during these events and related internal exercises, the Commission has refined a cyber incident response structure to facilitate identification and understanding of the impacts to communications from a developing cyber incident; conduct interagency coordination with other elements of the U.S. Government; and ultimately enable appropriate regulatory response including rapid approval of waivers, STAs, or other mechanisms to facilitate government and private sector response activities.



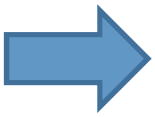
The Commission should continue to deepen relationships with the national security, law enforcement, and intelligence communities to identify and assess long- and short-term cyber risk. It should also continue efforts to enhance its internal process and capability to execute response, including hosting and participating in tabletop and other exercises involving federal and industry partners. CSRIC is a potential mechanism for industry to provide advice on potential waiver, STA, and other regulatory activity that may be needed very

rapidly during a significant cyber incident and should therefore be included in pre-planned response templates and primed for rapid execution.

### *Real-Time Cyber Threat Information Sharing*

Real-time cyber threat information sharing enables an ecosystem where indicators of attempted compromise can be shared in real time, protecting companies and agencies from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of exploits.

Again, presuming that market forces acting naturally can arrive at the most flexible and innovative solutions, the Commission has first asked CSRIC to identify and assess perceived technical and legal impediments to cyber threat information sharing, analyze potential solutions to the impediments, and develop recommendations that would enable real-time cyber threat information to be broadly shared across the communications sector.



Spotting and attributing successful cyber attacks is one of the most vexing challenges for information-intensive organizations. While DoD and the intelligence community recognized years ago that M2M information sharing and collaborative analysis are best practices, information sharing in the commercial sector between companies remains elusive. The FCC, with DHS and industry, should seek to change the corporate culture from one where fear of liability from sharing is replaced with a culture where M2M info sharing and collaborative analysis are accepted industry normative best practice. CSRIC will provide recommendations to the Commission in March 2017 that will offer guidance on how communications companies can effectively share cyber risk information pertinent to communications critical infrastructure within the private sector. The cybersecurity information under consideration will include non-real-time threat indicators and warnings, real-time anomalous indicators, and post-incident information related to cyber exploits on communications critical infrastructure. The Bureau will evaluate these recommendations and provide the Commission with a report that recommends which among them should be implemented and how the Commission can act to do so. In addition, smaller providers may have unique challenges with respect to information sharing. As explained above, the Commission should consider establishing, in partnership with relevant small provider industry associations, a funded ISAO Pilot Project for smaller providers.

### *Supply Chain*

Cyber risk can be introduced at any stage of the communications supply chain, from product design, to testing, to manufacturing, to product introduction and distribution, to product maintenance and support, and finally, to product retirement. Reducing risk in the communications supply chain requires the consideration of routine and exceptional risks introduced along the supply chain. Information and communications technology (ICT) products and services may contain malicious injects or leave us susceptible to higher risk due to poor manufacturing and development practices within the ICT supply chain. These risks come with the lack of understanding and control over how the technology is developed, integrated and deployed, as well as the processes used to assure the integrity of such products and services.

The FCC and our industry partners must focus on the mitigation of supply chain security and insider threat risks in the U.S. ICT sector. The FCC has taken a collaborative approach to cyber risk management, including supply chain risk management, by working in partnership with private-sector stakeholders through the CSRIC.

**Supply Chain Risk Management Forum**

Recognizing the significance of Supply Chain Risk Management (SCRM) and Insider Threat (IT) to the United States Information and Communication Technology (ICT) sector, the FCC partnered with the Office of the Director of National Intelligence (ODNI)/National Counterintelligence and Security Center (NCSC) to co-host a SCRM-IT Forum in July 2016. The industry participants included national providers and associations across the ICT sector to include wireline, wireless, broadcast, cable and satellite. In addition to the FCC and ODNI/NCSC, other government participants included DHS, DoD, FBI, NIST and NSA. The content focused on the identification, evaluation and mitigation of supply chain risks and insider threats to the ICT sector, and included sharing of best practice mechanisms for corporate supply chain risk management. Over 120 individuals representing industry and the government participated in a full day of information sharing to include material to assist companies with implementing effective SCRM and IT programs. Additionally, the FCC noted the intent to further share this information with small and medium-size providers through association events. The American Cable Association (ACA), representing nearly 750 small and midsized independent providers, was the first to contact the FCC to share this information through a webinar with their members in January 2017. Improving the SCRM and IT posture of the U.S. ICT sector is an imperative in ensuring the integrity of this critical infrastructure.

*Figure 7 - Supply Chain Risk Management Forum*

The Commission should consider continuing efforts to reduce supply chain risk and the risk from insider threats. Sustaining productive engagement with

telecommunications providers, the vendor community, and federal agencies with counterintelligence and supply chain risk responsibilities has significant risk reduction value.

### *Mergers and Acquisitions*

As cybersecurity risk management takes on greater importance in the overall management of corporate risks, and in light of recent cyber security threats and attacks, the Commission has in reviewing several recent major combinations examined cyber risk management as part of its statutory public interest determination. The Commission's review of cyber risk has focused on risk management plans and efforts for the potentially vulnerable transition periods when formerly independent networks are being integrated into a new enterprise. During the application review process, the Commission has asked for the applicants' current cyber risk management plans as well as their anticipated plan for the merged entity and makes use of the *2014 NIST Framework* as a way to evaluate the applicants' proposals. The Commission has required merged entities to submit information describing their cyber risk management plans. The Commission may impose a cybersecurity condition to the merger to help cure a potential public interest harm.

A recent example of how the Commission evaluated cyber risk in a merger context is Charter Communications' 2016 acquisition of Time Warner Cable and Bright House Networks. In that case, the companies entered the merger process with very different approaches to cyber risk management. The acquiring company, Charter, had elevated cyber risk discussions to very senior levels of the company and was already including cybersecurity as part of its governance framework to ensure that senior management and the board of directors are regularly briefed about cybersecurity issues and can make informed decisions.[34] It had adopted and was implementing the *2014 NIST Framework* as well as several practices identified by CSRIC IV and would apply these also to the new enterprise.[35]

Time Warner Cable, one of the acquired companies, provided cybersecurity updates to its Board of Directors, but also maintained a 24x7 Enterprise Risk Operations Center dedicated to supporting customer-facing security risks, including assisting customers with cyber threats.[36] Bright House, the other acquired company, stated that it employed safeguards to protect its network and customer information, including updates to management and had formed an internal council with C-suite/senior VP-level participation to improve executive visibility on information security risks, breaches, trends and training. Further, Bright House had a formed a dedicated

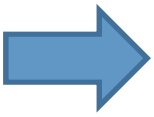
[34] *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership For Consent to Assign or Transfer Control of Licenses and Authorizations*, MB Docket No. 15-149, Memorandum Opinion and Order, 31 FCC Rcd 6327, 6519-20, para. 424 (2016) (Charter Merger Order).
[35] *Id. at* para. 423-24, and notes 1414-15, 1418.
[36] *Id. at* para. 425, and notes 1423-26.

security team reporting to the CIO to address, and had deployed distributed denial of service (DDoS) detection and mitigation security controls, robot network (BOTNET) sensors, and Web Application Firewalls.[37]

During the merger review, Charter told Commission staff that it had begun the process of identifying the "best of breed" cybersecurity practices at each company with the collaboration of the top cybersecurity personnel from each of the three companies. Further, Charter stated that it would establish a corporate governance structure to ensure that the merged entity's board and management were actively engaged in oversight and implementation of the company's cybersecurity program.[38]

The Commission recognized that the objective network goals outlined for the new entity would require proactive measures to reduce risk and protect consumer data and transactions. The Commission acknowledged in the Charter/TWC/Bright House transaction that the period of time during which combining companies are integrating operations poses increased risk, especially if either network is starting from a potentially weak network infrastructure, cyber protections or risk management plan.[39] "Increased complexity while in a transition state, changes in the cybersecurity workforce, the establishment of trust relationships between networks, and the continued evolution of tools used to attack networks together suggest a significantly raised cyber risk environment during the integration period."[40]

Ultimately, in the case of Charter, the Commission required the merged entity to submit a confidential filing to the Bureau within three months of the close of the transaction describing plans for managing the increased cybersecurity risks during the transition period.[41]



The Commission should continue to make cybersecurity risk management an element of merger reviews.

### *Technology Transition – IP Convergence*

Over the past decade, the growth of the Internet and broadband infrastructure has transformed the way society accesses information. The communications sector continues to experience a sweeping transition from circuit-switched voice communications to an all-IP environment. Wireless services and technologies have advanced dramatically. Communications have moved

[37] *Id. at* para. 426, and notes 1430-32.
[38] *Id. at* para. 427, and notes 1433-36.
[39] *Charter Merger Order*, 31 FCC Rcd at 6521-22, para. 429.
[40] *Id. at* para. 431, and note 1440.
[41] *See Charter Merger Order*, 31 FCC Rcd at 6552-53, Appendix B, Section VIII (Cybersecurity Security Plans Commitment).

from analog to digital, from voice-only services to wireless broadband, from 2G to 4G and now the promise of 5G which will support the continued growth of the IoT. These technology transitions, and the continued development of the IoT, create vast opportunities for businesses and consumers.

## Robocalling

Robocalls are unsolicited prerecorded telemarketing calls to landline home telephones, and all autodialed or prerecorded calls or text messages to wireless numbers, emergency numbers, and patient rooms at health care facilities. The security vulnerabilities that can lead to robocalls can also affect public safety communications networks, if successfully exploited. In particular, public safety stakeholders using legacy communications facilities are susceptible to call floods, which are large amounts of automatically generated calls directed at a single enterprise. These same call floods can lead to telephony denial of service (TDoS) attacks that can overwhelm enterprise voice network facilities and result in a shutdown of emergency services.

FCC rules limit many types of robocalls, though some calls are permissible if prior consent is given. The Robocall Strike Force, led by AT&T, was formed on August 19, 2016 in response to Chairman Wheeler's request that action be taken to eliminate robocalling. The Strike Force has contributed to the acceleration of new standards focusing on mechanisms to support Caller-ID validation. Furthermore, CSRIC has work in progress to improve the security of the underlying SS7 protocol, which has been used to set-up and tear-down communications circuits since the 1980s. Part of that work is determining the extent of any overlap between security flaws in the SS7 protocol and how those flaws can be exploited to conduct robocalls. Going forward, the establishment of a single Trust Anchor might provide a way to help verify caller IDs for SIP, SMS, and VoIP users.

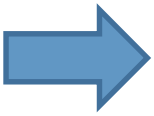
*Figure 8 - Robocalling*

However, with these new opportunities come new vulnerabilities. IP networks are multi-layered and more highly interconnected than legacy networks, which emphasizes the importance of interoperability. Information needs to travel seamlessly not only within networks but also between wide arrays of network types. New technologies, devices and networks often carry significantly more cyber risk than those they replace. For example, IoT devices introduce a significantly increased attack surface by orders of magnitude. Another example is ATSC 3.0 (discussed below). Strong cybersecurity policies and protections are crucial during these technology transitions to maintain the reliability and resiliency of communications services. Accordingly, given the critical importance of cybersecurity risk reduction during this period of IP convergence, the Bureau recommends that the Commission undertake a line of effort to address risk reduction across each of the five communications segments (satellite, wireless, wireline, broadcast, and cable).

## ATSC 3.0

The increasing integration of Internet-connected computer systems into broadcast station infrastructure exposes broadcast television systems to a new set of adversaries, willing and able to exploit these new attack vectors. A dramatic example is the 2015 attack on French broadcaster TV5Monde, where a nation-state actor hacker took control of its TV channels and hijacked its social media accounts. The new services and capabilities that the next evolution of broadcast television will introduce to the public, represented by the creation and adoption of ATSC 3.0 standards, will accelerate the integration of internet-exposed equipment, and the potential vulnerabilities associated with such connections, into broadcast television systems and into consumers' homes. ATSC 3.0 will establish an IP-based path into smart TVs receiving the broadcast that will have a high likelihood of direct interconnection with home Wi-Fi, Bluetooth, wireless, and wireline broadcast service. The significance of these potential vulnerabilities is amplified by the national security function of broadcast television as a method of distributing a Presidential Alert through the Emergency Alert System (discussed above).

*Figure 9 - ATSC 3.0*



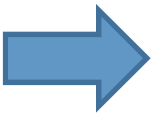
Since the new standards work on Caller-ID validation relies on the existence of Trust Anchors, the Commission should consider issuing a NPRM to improve Caller-ID validation and address SS7 security risks based on the recommendations from the Robocalling Strike Force and CSRIC. In addition, the Commission should consider developing a record on the steps that industry is taking to safeguard the confidentiality, integrity and availability of ATSC 3.0 broadcasting.

### *Workforce*

Cybersecurity professionals have unique skills, are in short supply, and are vital to our nation's security. As a result, competition for talent is fierce and establishing a strong team is essential. This requires organizations to tailor how they plan for their cybersecurity workforce so they have the right people in the right positions. In Executive Order 13636, Improving Critical Infrastructure Cybersecurity, the President assigned the Department of Homeland Security (DHS) the leadership role to work with Federal Agencies and sector specific regulators to help ensure the U.S. has skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders. One of the results of this mission is the collaborative effort with the National Initiative for Cybersecurity Education (NICE) that resulted in the development of the National Cybersecurity Workforce Framework (NCWF).

CSRIC was asked in March 2015 to examine and develop recommendations regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. CSRIC was asked to consider means to promote a common lexicon and roadmap that will promote more effective interfaces with academic institutions and other training environments. CSRIC will deliver its final recommendations in March 2017.

Bureau staff have worked with the National Science Foundation's Scholarship for Service program to advance professionalization of the cyber workforce, and have hired SFS scholars to serve at the Commission. The Bureau has also engaged with the National Security Agency's Centers for Academic Excellence (CAE) program office to advance communications sector and public safety sector needs when considering criteria for designating two- and four-year academic institutions as CAEs in cybersecurity operations. Finally, staff have leveraged multiple opportunities to advance direct outreach with academic institutions supporting cybersecurity education initiatives. For example, Bureau staff have worked with the University of Colorado-Boulder and the University of Kansas to put on cybersecurity workshops, spoken at cybersecurity events and competitions such as the CyberSEED event at the University of Connecticut and a policy speaker series at the Taubman Center for American Politics and Policy at Brown University, and conducted direct engagement with leading cybersecurity institutions such as Carnegie Mellon University.



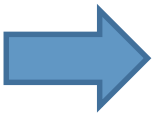
The Commission should consider developing a process to support a periodic review and update of the knowledge, skills and abilities of cyber professionals needed by the communications and public safety sectors. The Commission should also consider mechanisms for messaging these needs from industry to academia, and vice versa.

### *International Outreach*

Our interconnected networks extend beyond our borders, as do cyber risks. Commission staff works on outreach activities to share ideas and results with other governments. Commission staff reaches out to international stakeholders through regular visits to the Commission where ideas are exchanged about the different approaches to cyber risk management. In 2016, Bureau staff met with representatives from numerous countries as part of the Department of State International Visitor Leadership Program and the FCC's International Visitor's Program to discuss the FCC's "trust but verify" approach to cybersecurity risk management, endorse multi-stakeholder Internet governance and provide technical presentations and discussions led by the Bureau's subject matter experts.

As part of the Department of State Global Connect Initiative Technology Leadership Program, Bureau staff also participated in a Network Security Workshop in India in October 2016, to discuss the Commission's market-based approach to cyber risk management. Finally, the Commission plays a lead role in the yearly US Central Command (CENTCOM) Regional Cybersecurity Conference (CRCC). The CRCC supports the ongoing dialogue on cybersecurity related matters between our government and regional partners.[42] Participants from each country include representatives from the military, the diplomatic corps and telecommunications ministries and regulators. The relationships built through the annual CRCCs assist CENTCOM in creating a more stable and prosperous region with increasingly effective governance, improved security, and trans-regional cooperation to counter state and non-state actors posing a threat to U.S. interests.[43]

The FCC has been engaged in "whole of government" activity to address risk in the telecommunications sector with our closest allies, recognizing the importance of balancing marketplace considerations with national security objectives. We met with the U.K., Canada, New Zealand, and Australia in 2015 at the Five Nations Technology Summit. The Summit, hosted by the British, brought together a cross section of government officials and technology experts from these five English-speaking nations to address emerging trends in the security space and further a best practice mindset in answering challenges – both present and future.



The Commission should continue to work to achieve greater harmonization between regulators and security agencies in other nations.

## Conclusion

The security and resiliency of the nation's communications infrastructure is vital to emergency services, national security, and our very way of life. Since the vast majority of the commercial communications infrastructure is in private hands and private actors act first to maximize shareholder value, there is residual risk that remains when a firm's risk tolerance exceeds that which is in the public interest. This is particularly so when consumers are not aware of the risk they are being asked to bear. Firms that internalize more risk are placing themselves at a competitive advantage as they forego cybersecurity investments and lower the cost of their goods and services. Residual risk in the commons presents perverse market incentives. Those firms that internalize less risk expose themselves to a loss of market share. Looking forward, the continued convergence of packet-based communication technology in wireless, wireline, cable, broadcast and satellite coupled with network functional virtualization and software defined

[42] Countries with in US Central Command region include Egypt, Jordan, Syria, Iraq, Iran, Saudi Arabia, Yemen, Qatar, Oman, UAE, Pakistan, Afghanistan, Turkmenistan, Uzbekistan, Kyrgyzstan, and Kazakhstan.

[43] *See* http://www.centcom.mil/ABOUT-US/

radios will lead to hybrid (co-mingled) control elements for many service providers. These interdependencies will be inviting targets for threat actors from nation-states, to criminals, to hacktivists wishing to exploit or disrupt critical infrastructure. The holistic nature of the interdependent services and exposed attack surface suggest that an "all hands on deck" approach for residual risk, utilizing the full range of government expertise and authorities working with commercial providers, is appropriate. This document presents a strategy to promote an acceptable balance between corporate and consumer interests in cyber risk management when elements of market failure are at work. It acknowledges that the Commission's preference is to work collaboratively with industry using private/public partnerships. However, if market forces do not result in a tolerable risk outcome, the Commission has tools available to make adjustments to restore the balance.

# Appendix A

## FCC Authorities for National Security & Cybersecurity

January 2017

**The Federal Communications Commission**

- An independent regulatory agency
    - Primary and plenary authorities over telecommunications

**Communications Act, Section 1**

- FCC established in part "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications."
- Section 1 informs and buttresses the Commission's exercise of its authority under the specific provisions Communications Act.

**Communications Networks**

- Broad authority over communications common carriers:
    - Telecommunications
    - Broadband Internet access service (ISPs)
    - High-speed business data services
- FCC may implement cybersecurity or other measures:
    - Prescribe "practices" that are "just and reasonable" (§ 201)
    - Condition authorizations on "such terms and conditions as in its judgment the public convenience and necessity may require"; require carrier to "provide itself with adequate facilities" to perform its service (§ 214)
    - Require carrier to "protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers" (§ 222)
    - Require carrier to ensure that interceptions within its network "can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission" (CALEA)

**Radio Transmissions**

- Broad authority:
    - Includes, but not limited to, broadcasters (TV/AM/FM)

    - Includes all non-federal-government radio communication or transmission of energy
- FCC may require cyber or other measures as condition of license under its statutory authorities:
    - Allocate spectrum "in the public interest"
    - "Prescribe the nature of the service to be rendered"
    - Modify existing licenses if "such action will promote the public interest, convenience, and necessity, or the provisions of this Act or of any treaty … will be more fully complied with."

**Equipment Authorization**
- FCC must authorize radiofrequency (RF) devices prior to their being marketed or imported into the United States
- FCC determines the standards that equipment must meet to obtain authorization, *e.g.*, RF interference potential; compliance with rules that address other policy objectives
- Could include cybersecurity measures

**Public Safety Reporting**
- FCC shall investigate and study "all phases" of "obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property,… and the best methods of obtaining the cooperation and coordination of these systems." (§ 4(o))

**War Powers**
- Section 706 grants powers to the President in the event of war, threat of war, state of public peril or disaster, or national emergency.
- Presidential authority:
    - Prioritize essential communications
    - Suspend or amend FCC rules (within FCC authority)
    - Close facilities or radio stations
    - Authorize governmental use or control of stations or equipment
- This authority can be delegated "through such person or persons as he designates for the purpose, or through the Commission."

**Others Sources of Authority**
- "Ancillary authority" to regulate interstate wire and radio communications if necessary to accomplish other statutory objectives (§ 154)
- Wireless Communications and Public Safety Act (E911)
- Authority to promote broadband deployment (§ 1302)
- Authority to revoke or condition licenses for undersea communication cables "to promote the security of the United States" (§ 35 & Exec. Ord. 10530)
- Warning, Alert, and Response Network Act (alerting)

**Non-Regulatory Activities**
- Convening industry
    - Industry engagement (C-suite and operational contacts)

- Advisory committees
    - Communications Security, Reliability, and Interoperability Council:
        - Evolving 911 Services
        - Emergency Alerting Platforms
        - Emergency Alert Systems
        - Submarine Cable Resiliency
        - Network Timing Single Source Risk Reduction
        - Cybersecurity Information Sharing
        - Secure Hardware and Software - Security by Design
        - Cybersecurity Workforce
        - Priority Services
        - Wi-Fi Security
        - Legacy Systems and Risk Reduction
    - Technological Advisory Council
        - Cybersecurity Working Group (NFV/SDN, 5G)
    - Robocall Strike Force
    - Task Force on Optimal PSAP Architecture
- Other industry collaboration
    - Wireless resilience commitments
    - Cyber assurance
- Interagency Coordination
    - Aviation communications interagency working group
    - IMSI catcher task force
- Public Safety Communications
    - 911, spectrum, alerting, NS/EP priority communications
- Harmful interference resolution
- High Frequency Direction Finding
    - Purposeful Interference Resolution Taskforce (PIRT)
- Enforcement Bureau with field offices
- Engagement with federal agencies
    - Chair of the Regulator's Cybersecurity forum
    - Test and operation of special systems (RF, C-UAS, IMSI, C-IED)
    - NSC and OSTP
    - Engagement with state and local agencies & regulatory bodies
- Merger and acquisition review, conditioning, and/or approval for the telecommunications market
- International
    - Rules for foreign company participation in the US communications market
    - Bilateral engagement with other national regulatory authorities
    - International Telecommunication Union (ITU) and standards bodies

# Appendix B

## The Market for ISP Cybersecurity

**FCC Public Safety and Homeland Security Bureau**

**Staff Report**

**December, 2016**

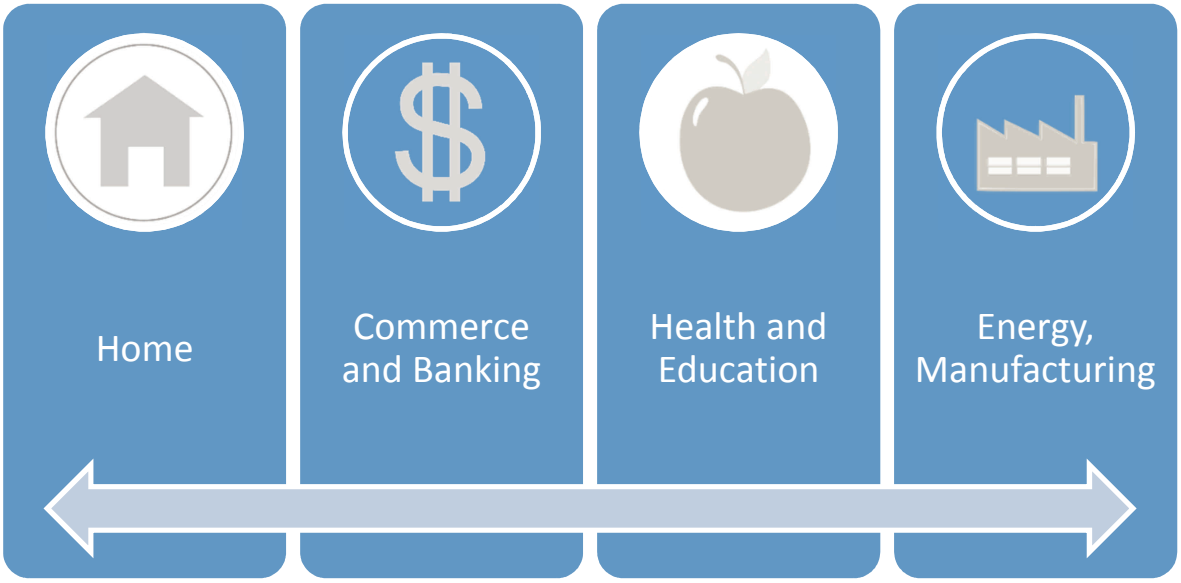
Malicious activity threatens the availability and reliability of the communications critical infrastructure. While the private sector continues to invest in cybersecurity, investment may not be socially optimal due to the presence of market failure.

Significant economic literature exists on the subject of cybersecurity and market failure. Cybersecurity policy discussions, however, often focus on engineering and legal issues without discussing the impact of market failure on entities' incentives to invest in more secure systems. This paper seeks to fill this gap, presenting the implications of economic reasoning for solving some persistent cybersecurity problems.

To begin, this paper explains the economic concept of market failure. Market failures include externalities, the presence of market power and information problems. Examples are provided to cement the reader's understanding. This review of market failure underscores the possibility that some persistent problems may not be addressed by the market alone.

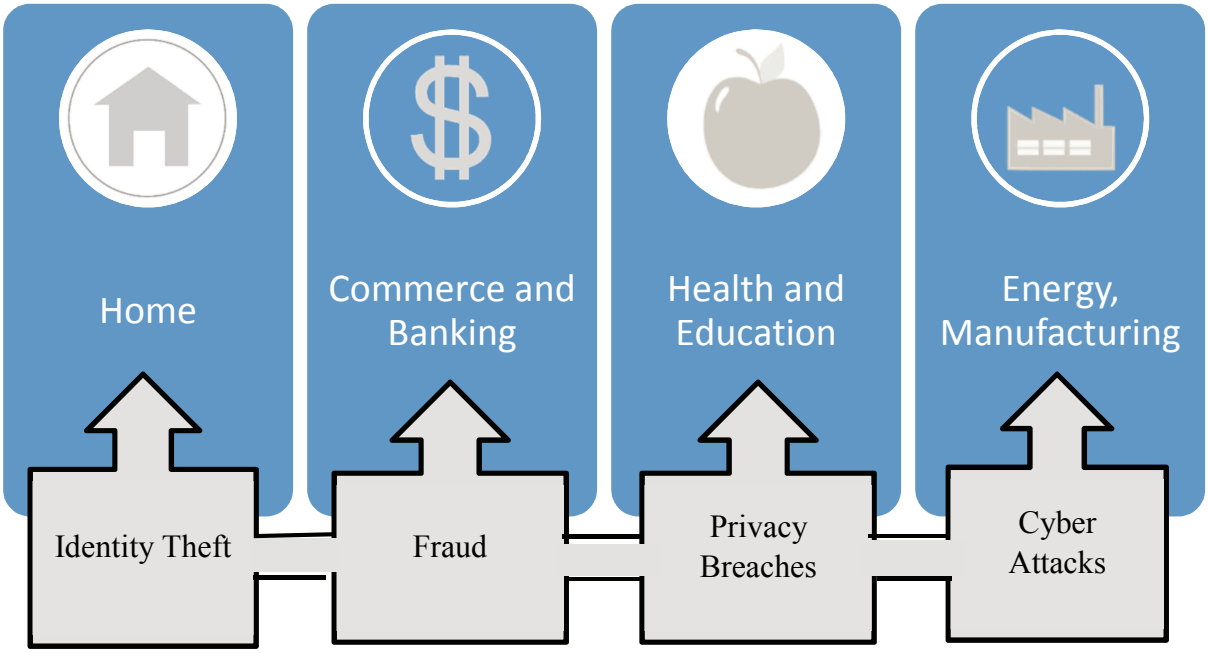
Next, this paper examines potential market failures in Internet Service Provider (ISP) cybersecurity. FCC investigation to confirm the presence and severity of market failure, and examination of policy options may be necessary to improve the cybersecurity of the communications critical infrastructure.

**The Internet has become a Central Feature across our Economy.**




The Internet has facilitated tremendous gains for the U.S. economy. Internet use continues to grow as a large majority of U.S. adults use the Internet for work, health care, education and entertainment.[i] E-commerce has grown steadily for the past decade.[ii] Seventy-one percent of consumers bank online.[iii] Telemedicine has also grown rapidly.[iv] Digital learning is transforming education.[v] The smart grid and other advances in the energy sector are enabled by the Internet.[vi] Connectivity is speeding up manufacturing and improving plant safety.[vii] The public's trust in the Internet, however, is under stress.[viii]

**Cybersecurity Challenges are Common.**




Every sector is grappling with cybersecurity problems. Identity theft complaints to the FTC increased more than 47 percent in 2015, compared to 2014.[ix] Cybersecurity incidents are becoming more destructive.[x] Distributed Denial of Service (DDoS) attacks are increasing in number and intensity.[xi] Data breaches in healthcare are common, and becoming more frequent.[xii] Universities have also sustained damaging cyber breaches.[xiii] Manufacturing companies are experiencing sophisticated attacks that bypass their standard security measures.[xiv] The energy and utility sectors have suffered major financial losses as a result of cybercrimes.[xv] The trend line of cybersecurity problems is not reassuring.

**Telecommunications Cybersecurity Challenges and the Role of ISPs**

In connecting consumers, businesses and government to the Internet, ISPs provide much value to our nation. The Internet carries much legitimate traffic, but it also carries harmful traffic. The volume of harmful traffic is growing. Malicious botnets generate 30 percent of Internet traffic – a portion that shows no sign of shrinking.[xvi] Enterprises report that defending their systems against malware is becoming harder, not easier.[xvii]

Consumers, devices and apps at the edge of ISP networks are not well defended. Consumers are "leaving their digital doors unsecured," failing to protect their security and privacy.[xviii] Vulnerabilities in the Internet of Things that have been exploited in recent months could have been avoided if industry best practices had been followed.[xix] Mobile applications have significant security flaws.[xx]

ISPs could counter some of these vulnerabilities by adopting more secure Internet protocols, monitoring and filtering traffic, and alerting edge users to evidence of malware infections. Why might ISPs not adopt cybersecurity measures that are appropriate for the modern threat environment? The answer to this question, from an economic point of view, is complex.[xxi] Economic theory can point to several possible sources of difficulty. Let us begin with a review of how markets work, and how they sometimes fail.

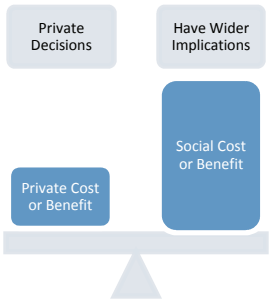
*A market economy relies on the "invisible hand" of self-interest and competition to maximize social welfare.*

**How Markets Work**: Over 200 years ago, economist Adam Smith described the market economy as a system where self-interest and competition are the "invisible hand" that guides resources to their best use. "It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest."[xxii] A baker provides bread for sale – not for the good of society, but in his self-interest to feed his family. One might ask, will self-interest not lead the baker to set very high prices for his bread? Smith explained that self-interest is held in check by competition. If a baker sets the price of bread too high, or provides poor quality or service, a self-interested neighbor might see an opportunity for profit, and open a competing bakery. This tension between self-interest and competition results in an "invisible hand," which leads people to make decisions that drive resources to their most valuable use – an efficient allocation. Where markets function properly, no government intervention may be necessary.[xxiii]

**How Markets Fail**: While markets can provide fertile ground for innovation and productivity, they sometimes fail to allocate resources efficiently. The Office of Management and Budget describes three major types of market failure that could call for regulation: externalities, market power and inadequate or asymmetric information.[xxiv]

- **Externalities** - Costs and benefits of a transaction that are not absorbed by the buyer and seller, but accrue to third parties.[xxv]
- **Market power** - The ability of an individual buyer or seller to influence the availability or the market price of a good or service.
- **Inadequate or asymmetric information** - The lack of relevant information to one or both parties in a transaction.

The market for ISP cybersecurity may suffer from one or more of these three market failures, as discussed below.




*Externalities are impacts on third parties.*

### *A. Market Failure #1: Externalities*

A market transaction has externalities when the actions of one agent impact other agents that are not a party to the transaction. Externalities impede the ability of markets to achieve outcomes that are optimal for society as a whole when agents do not fully consider third-party impacts.

Externalities can be positive or negative. Pollution is a classic example of a negative externality. A factory that generates pollution has a negative impact on third parties – those affected by the pollution. Factory operators consider many costs of production, but markets do not generally require them to consider the costs of pollution borne by third parties. If they had to bear these costs, they would tend to either produce less product, or produce their product in a way that generated less pollution. Markets tend to over-produce goods and services with negative externalities.

Government action can counter the inefficiencies caused by negative externalities, moving the market toward what would be optimal for society. Mandatory standards or other rules or fees can decrease the production of goods and services with negative externalities. Audits or examinations can promote the adoption of best practices to mitigate negative externalities. The government can provide liability protection in exchange for actions that otherwise could increase a firm's legal risk.[xxvi] It can assign liability to the party most able to address the externality.[xxvii]

Externalities can also be positive, as in the case of education and healthcare. Educated, healthy individuals are more productive and safer to be around. Society – not just the individual – benefits from quality education and health care. A market will tend to produce too little of goods and services with positive externalities because the third parties that benefit do not help fund the provision of such goods and services. The government can promote the provision of such goods through subsidies or tax incentives.[xxviii] Other options include regulation (such as requiring immunizations) and direct government provision (such as public education).

**FCC Action Related to Externalities**

Whether positive or negative, externalities are one of the classic market failures that may justify government intervention. The FCC's broadband promotion policy, for example, was motivated by the presence of positive externalities associated with broadband adoption, including the promotion of telework and access to education and healthcare.[xxix]

**How do Externalities Impact Internet Cybersecurity?**

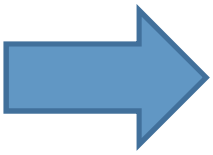
Externalities are common in the market for ISP cybersecurity because one party's network security practices can impact third parties. For example:

***Secure Internet Protocols***: The Internet has systemic security problems because it was designed to assume mutual trust among users. Standards bodies have agreed upon several protocols to improve Internet security to combat threats introduced by untrustworthy users. Some of these protocols have significant positive externalities (their benefit to society exceeds their benefit to individual ISPs), and thus they have enjoyed less-than-societally-optimal adoption. Protocols like DNSSEC provide little or no protection to early adopters, but could have a significant impact if all ISPs adopted them. While most U.S. government agencies have deployed DNSSEC, most ISPs (with the exception of Comcast and Sprint) have not.[xxx] BGPSEC is an Internet routing security protocol with a similar problem: it has not been widely adopted because there are no benefits for early adopters.[xxxi] Insufficient incentives may exist to promote ISP adoption of more secure Internet protocols like DNSSEC and BGPSEC because those protocols have significant positive externalities and they require wide adoption to work well.

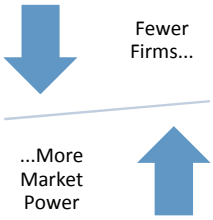
***Cyber Hygiene***: Good cyber hygiene has a positive externality. It decreases risks to third parties by making malware less prevalent. End-users could reduce the flow of malware through the Internet by practicing good cyber hygiene. Some end-users do limit their risky behavior and purchase cybersecurity protection, but in doing so, they are likely only to consider their own protection – not the protection of society at large.[xxxii] That is, end-users tend to take more risks and purchase less protection than would be socially optimal.[xxxiii] Evidence suggests that end users often fail to update their malware protection.[xxxiv] End-users may have insufficient incentives to maintain cyber hygiene habits that are optimal for society.

***Strong Authentication***: Strong passwords and the use of multi-factor authentication are practices that have positive externalities. Strong authentication practices can protect both consumers and their credit card companies from fraud in e-commerce. They can also protect employees and their employers from breaches. We can expect sub-optimal authentication practices from Internet users, however, because some of the positive impacts of this behavior accrue to third-parties. Evidence supports this hypothesis. In 2015, for example, 63% of confirmed data breaches involved weak, default or stolen passwords.[xxxv]

***Cyber Education***: Education, including education about cybersecurity, has positive externalities. The private sector demand for cybersecurity education only reflects the expected financial rewards to the individuals being trained – not the external rewards to society at large. Despite a well-known shortage of cybersecurity workers, the majority of top-ranked American undergraduate universities are not prioritizing cybersecurity as a requirement for computer science undergraduates.[xxxvi] The federal government, recognizing the need to promote cybersecurity education, established the National Initiative for Cybersecurity Education (NICE), a partnership between government, academia and the private sector.[xxxvii] The Department of Homeland Security promotes cybersecurity awareness, training and education through the National Initiative for Cybersecurity Careers and Studies (NICCS).[xxxviii] It also provides free cybersecurity training to the entire government workforce.[xxxix]



Externalities can impact cybersecurity. More research is called for to determine the extent of this impact. Intervention may be justified.




*A firm with few or no competitors has market power.*

### *B. Market Failure #2: Market Power*

Recall that competitive forces – the presence of many firms competing with each other – can drive resources to their most efficient use. If one firm sets prices too high, or makes low-quality products, competitors will enter the market to drive prices down and drive quality up. Sometimes, however, competitors may not enter the market. If there are barriers to market entry, a market may be served by only one firm (monopoly) or a small number of firms (oligopoly). In such cases, the firm or firms in the market are said to have market power.[xl] Firms with market power can set prices too high or produce lower than optimal quality without fear of competition. Firms with market power are said to be "dominant providers."

> Market power refers to the ability of a firm (or group of firms) to raise and maintain price above the level that would prevail under competition. The exercise of market power leads to reduced output and loss of economic welfare. – OECD[xli]

Classic regulatory responses to market power include regulating the prices or output of a monopolized industry, such as a water, electricity or telephone service. Or the regulator might break up a monopoly and introduce competition.

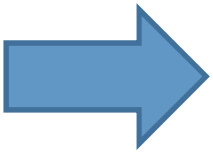
**FCC Actions Related Market Power**

The FCC has taken several actions relating to market power. For example, in its spectrum auctions, the FCC established a market-based spectrum reserve in connection with the Incentive Auction designed to prevent excessive concentration of spectrum holdings while promoting competition for spectrum.[xlii] The FCC has also worked with the wireless industry to reduce the scope, incidence, and impact of cell phone "locking," which tied consumers for long periods to one wireless service provider.[xliii]

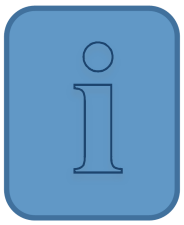
The FCC has also addressed market power in its 2010 Open Internet Order, and its subsequent 2015 Order, aimed at ensuring that broadband providers do not privilege their own vertically integrated content, discriminate against others' content, or force content providers to pay fees for access or preferential access to customers. In other words, broadband providers should not exploit their "terminating access monopoly." [xliv]

**How does Market Power Impact the Market for ISP Cybersecurity?**

Fifty-one percent of Americans have access to only one fixed broadband provider.[xlv] The ISP market has high entry costs, a factor that may contribute to ISP market power.[xlvi] The small number of Tier 1 networks also weakens the ability of other ISPs to "shop around" for more secure Tier 1 networks with which to exchange traffic.[xlvii] With little competition, there may be little incentive for ISPs to invest in cybersecurity, and there may be little chance for consumers to choose an ISP based on security considerations.[xlviii]



Market power may have a negative impact on ISP cybersecurity. More research is called for to determine the extent of this impact. Intervention may be justified.



*Information problems may be common in the market for ISP cybersecurity.*

### *C. Market Failure #3: Imperfect Information*

Another source of market failure is imperfect information. For markets to work smoothly, parties to transactions must have the information they need to make optimal choices. When two parties to a transaction do not have equal access to information – or if they both lack relevant information – the transaction may not be optimal.

Government can improve the availability of information in many ways. For example, setting standards and requiring certification can help customers determine the value of a product or service. The government can also promote information sharing by providing antitrust protection, by acting as a convener, or by requiring information sharing. Where an expert third party is able to glean relevant information, the government can encourage publication of such information in order to inform the market. Government agencies can also provide information directly to the public.

**FCC Actions Related to Imperfect Information**

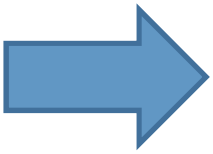
The FCC provides informational resources to consumers and small businesses. The Consumer Affairs and Outreach Division (CAOD) engages the public through outreach and education initiatives to inform them about important consumer-related regulatory programs, telecommunications issues and other consumer issues that impact their day-to-day life.[xlix] In early 2016, the FCC launched a voluntary broadband labeling program to help consumers make informed choices among broadband plans. The FCC also helps small businesses create customized cybersecurity plans, and provides a cybersecurity tip sheet for small businesses.[l] In 2015, the FCC improved the ability of Public Safety Answering Points to accurately identify the location of wireless 911 callers.[li]

**How do Information Problems Impact the Market for ISP Cybersecurity?**

Information problems in ISP cybersecurity may include both a lack of information about cyber threats and informational asymmetries.

***Lack of Information***: Even for the most advanced organizations, many cyber threats are not fully known because new threats continue to emerge. Information about known threats is not widely shared because of reputational and litigation risk. Therefore, precisely measuring the level of security of information systems is not possible.[lii] ISP efforts to secure their networks are impeded by this lack of information. This general lack of information also reduces confidence in the Internet.

***Informational Asymmetry***: Informational asymmetries are widespread in the market for cybersecurity.[liii] For example, consumers are less willing to pay the full value for ISP security because they cannot verify an ISP's security claims.[liv] Similarly, consumers may purchase sub-optimal amounts of malware protection because they cannot discern its quality or value. Given this market failure, ISPs find it difficult to compete on security claims, and may have difficulty recouping the cost of security enhancements. Information sharing, transparency, labeling, and the provision of consumer information may help address the problems.

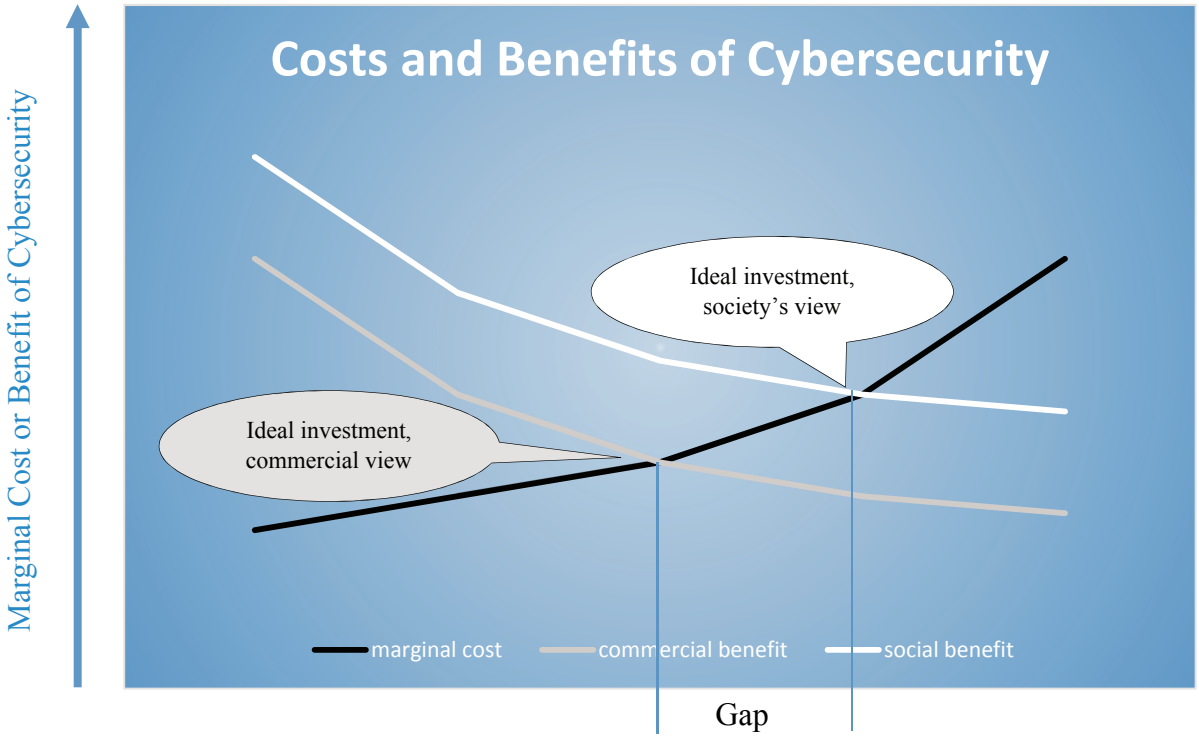


Information problems may be common in the market for ISP cybersecurity. More research is called for to determine the extent of information problems. Intervention may be justified.

*Market failures may suppress ISP cybersecurity.*

**Market Failures may lead to Worsening Shortfall of Cybersecurity Investment**

Market failures such as externalities, market power and information problems may contribute to a market with a less than ideal level of ISP cybersecurity. As the graph below shows, firms make decisions that strike a balance between the costs and benefits of cybersecurity investments for themselves. But they do not consider the additional benefit to the public at large of investing in cybersecurity. The result is a gap in cybersecurity preparedness that the market, on its own, is unlikely to fill. The well-being of society at large would be improved by more investment, as



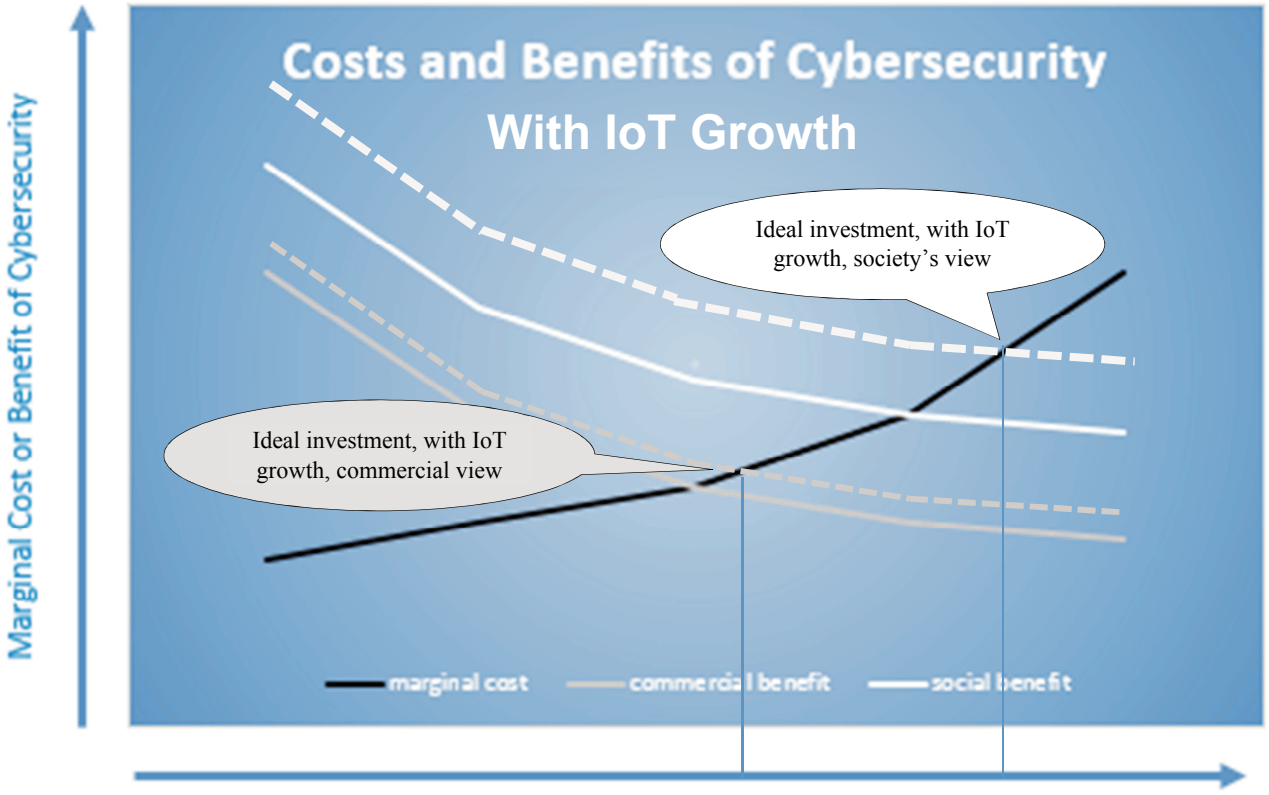
shown.

Cybersecurity Preparedness

**The Internet of (Insecure) Things Widens the Gap**

The burgeoning – and insecure – Internet of Things (IoT) market exacerbates the shortfall of cybersecurity investment. In late 2016, the Department of Homeland Security issued strategic principles for securing the IoT, and called on the public and private sectors to work together to improve IoT security.[lv]

Because of demonstrated negative externalities – third parties impacted by insecure IoT – the private sector alone may not have sufficient incentives to invest in cybersecurity.[lvi] The attack surface offered by the IoT is growing rapidly, calling for concerted effort to improve security.[lvii] Multiple network providers are impacted by the IoT, rendering a consistent response difficult. In addition, the multiplicity of price-competitive vendors hinders concerted efforts to build in voluntary security by design into the IoT. The graph below illustrates the widening gap between the ideal investment from the commercial point of view and society's view, with the growth of IoT. Many sectors are vulnerable due to this gap, as the IoT expands in public safety communications, industrial control systems, the use of machine-to-machine sensors, smart city technology, and broadband-dependent critical infrastructure.



More research is called for to determine the extent of each Gap type of potential market failure. The results of that research may militate for action – by voluntary industry associations and/or by the government.

**Residual Risk**

Firms decide on the ideal investment in cybersecurity preparedness by comparing the benefit of additional investment to the cost of that investment. As long as the expected benefit exceeds the cost, they will continue investing. However, as investment increases, marginal benefits decrease until, at some point, the firm calculates that additional investment would not be justified. Residual risk remains, but firms determine that the cost of mitigating that risk is too high: they accept the risk.

As shown in the previous section, the ideal level of cybersecurity investment from the firm's point of view is lower than the ideal level from society's point of view. Firms do not take into account the impact of their investments on third parties, nor are they able to solve some of the information problems inherent in cybersecurity. From society's point of view, it would be ideal to address some of the residual risk that remains after firms make their investment decisions.

A number of things can be done to address residual risk, either accepting the current level of risk or moving cybersecurity preparedness towards the level that would be ideal for society at large:

- Accept – The first option is to accept the residual risk that remains after marketplace participants make their investment decisions. This leaves third parties to cope with the risks imposed by others, but marketplace solutions may arise to help them. For example, security firms may create software to defend endpoints against DDoS attacks employing the IoT. As risk is transferred to third parties, costs are borne by third parties. But if these costs are low, risk acceptance may be a better option than intervention.
- Insure – Where information problems are significant, insurance may help bridge some of the gap. As insurers gain expertise, they may insist on increased cybersecurity preparedness in exchange for taking on the financial exposure that firms face from cybersecurity risk.
- Invest – Increased investment, beyond that which the market provides, can mitigate some of the residual risk. This investment could be undertaken by the government, consumers, or by providers themselves. Additional incentives would be required to motivate investment. That motivation could be provided by industry standards, reporting requirements, political pressure, or regulation.
- Transfer – Risk to third parties could theoretically be transferred to Internet Service Providers, if providers were held liable for risks imposed on consumers and others. This

would solve the externality problem, but could create a moral hazard problem: consumers and others would no longer have a strong incentive to protect themselves.

Policy makers will have to grapple with how best to handle the gap between the market's level of cybersecurity preparedness and the level that would be ideal for society.

**The Role of the ISP Industry**

ISPs are uniquely positioned to address malware and breaches, for their own operations as well as in support of other sectors. Should ISPs be asked to bear responsibility for the cybersecurity of their customers? Sloan and Warner give several justifications for shifting some of the responsibility for malware defense to ISPs, which have much more cybersecurity expertise than their customers.[lviii] Traffic enters and exits the Internet through an ISP, placing them in a good position to scan for malware. ISPs can monitor customers' traffic to detect bot infections. ISPs can also detect whether their customers are using unpatched versions of operating systems, browsers and plug-ins. ISPs, then, can take the leading role in cybersecurity for their customers. Evidence suggests that this trend has already begun. Organizations are asking more from their ISPs, including filtering network traffic and providing analytics for detecting existing problems and predicting imminent threats.[lix]

In Austria, Finland, Germany and Japan, where ISPs are active in monitoring traffic and addressing botnets, malware infection rates are lower.[lx] The U.S. is beginning to call on ISPs to take a more active role. In 2012, the FCC's CSRIC voted to approve the Anti-Bot Code of Conduct for ISPs.[lxi] Under the code, ISPs agreed to engage in activities to educate end-users, detect botnet activity on the network, notify customers with suspected botnet infections, provide information or directly assist in remediation of botnet infections, and collaborate with other ISPs in Code of Conduct activities.

In 2014, a group of network operators, with the support of the Internet Society, suggested a list of norms that would improve the resilience and security of the Internet. The Mutually Agreed Norms for Routing Security (MANRS) provides detail on these norms.[lxii] Participants include Comcast and Level3.[lxiii] The group is exploring how to verify that participants are actually adopting the suggested practices through compliance testing (where possible) and vouching.[lxiv]

**The Government's Role**

Industry groups and public-private partnerships can make a difference. Government action could be considered, however, if private sector groups are unable to enforce their agreements.

Both the potential for market failures in the market for ISP cybersecurity, and the need for a reliable communications networks may lead to consideration of government intervention. To date, the government has partnered with industry in various public-private partnerships, and taken action to secure government networks. Berkowitz and Hahn assert, however, that the government is not doing all that it can. U.S. government cyber strategy "rejects regulation, government standards, and use of liability laws to improve cyber security in toto. These are all basic building blocks of most public policies designed to shape public behavior, so one must wonder why they are avoided like a deadly virus (so to speak)."[lxv] Fred Cate and his coauthors claim that "[w]ithout more appropriate standards and oversight, we will never achieve the broad accountability that effective cybersecurity requires."[lxvi]

Government intervention should only be undertaken with care. There is currently a dearth of information to inform the appropriate form and scope of such an intervention. The first task is to examine existing information on the extent of market failure and consider additional information gathering efforts. If market failure is revealed, tailored intervention may be needed to address market failures and to address public safety concerns.

**Next Steps: What Actions Might the FCC Take to Address Market Failures?**

One responsibility of government is to address market failures. A Treasury Department report provides a list of potential government incentives that could improve the Nation's cybersecurity posture, including the use of regulation, where appropriate.[lxvii] The FCC and DHS, as well as NIST, FTC, NSA and the FBI could be well positioned to improve ISP cybersecurity.

The FCC is in a unique position to work with the ISP industry and other stakeholders because of our longstanding public-private partnership with the Communications Security, Reliability and Interoperability Council (CSRIC). Our work with CSRIC to provide voluntary guidance is a good start, but the rising threat of cybersecurity breaches may require regulatory action to improve network cybersecurity by counteracting market failures.[lxviii] Further research is necessary to provide visibility into the nature and extent of market failures in the market for ISP cybersecurity.

[i] *See* Andrew Perrin and Maeve Duncan, *Americans' Internet Access 2000 – 2015*, PEW RESEARCH CENTER (Jun. 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/; *cf.* Monica Anderson and Andrew Perrin, *15% of Americans Don't Use the Internet. Who are they?*, PEW RESEARCH CENTER, (Sep. 7, 2016), http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they/.

[ii] *See* Rebecca DeNale and Deanna Weidenhamer, *Quarterly Retail E-Commerce Sales 2nd Quarter 2016*, U.S. CENSUS BUREAU (Aug. 16, 2016, 10:00am, EDT), https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[iii] *See* Report, Board of Governors of the Federal Reserve System, Consumers and Mobile Financial Services 2016 (March 2016), *available at* https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf (stating that 71 percent of consumers used online banking in 2015).

[iv] *See* Krista Drobac, *2015: Another Unstoppable Year for Telehealth*, THE INSTITUTE FOR HEALTHCARE CONSUMERISM, http://www.theihcc.com/en/communities/health_access_alternatives/2015-another-unstoppable-year-for-telehealth_i7gjbohl.html (last visited Nov. 16, 2016).

[v] *See* Neil Campbell, *How Digital Learning is Transforming Education*, U.S. CHAMBER OF COMMERCE FOUNDATION (2016), https://www.uschamberfoundation.org/blog/post/how-digital-learning-transforming-education.

[vi] *See* The PEW Charitable Trusts, THE SMART GRID: HOW ENERGY TECHNOLOGY IS EVOLVING (Feb. 2016), http://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/02/the-smart-grid-how-energy-technology-is-evolving.

[vii] *See* Kylie Jane Wakefield, *How the Internet of Things is Transforming Manufacturing*, FORBES (Jul. 1, 2014, 11:51am), http://www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-is-transforming-manufacturing/#39debf9e228e.

[viii] *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activitie,* National Telecommunication & Information Administration (2016), *available* at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[ix] *See* Press Release, Federal Trade Commission, FTC Releases Annual Summary of Consumer Complaints (Mar. 1, 2016), *available at*https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints.

[x] *See* Charles Beard, et al., *US Cybersecurity: Progress Stalled. Key Findings from the 2015 US State of Cybercrime Survey*, PRICEWATERHOUSECOOPERS (2015), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[xi] *See* Verisign, VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT, VOLUME 2, ISSUE 4, 4TH QUARTER 2015 (2015), https://www.verisign.com/assets/report-ddos-trends-Q42015.pdf.

[xii] *See* PONEMON INSTITUTE, *SIXTH ANNUAL BENCHMARK STUDY ON PRIVACY & SECURITY OF HEALTHCARE DATA* (2016), *available at* https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents; *see also* SYMANTEC, INTERNET SECURITY THREAT REPORT (2015), *available at* https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

[xiii] *See* D. Frank Smith, *Putting 2015's Higher Education Cyberattacks into Perspective*, EDTECH (Sept. 23, 2015), http://www.edtechmagazine.com/higher/article/2015/09/putting-2015-s-higher-education-cyberattacks-perspective.

[xiv] *See* David Greenfield, *4 Types of Cyber Attacks Targeting Manufacturers*, AUTOMATION WORLD (Aug 20, 2015), http://www.automationworld.com/4-types-cyber-attacks-targeting-manufacturers.

[xv] *See Cybersecurity Policy and Threat Assessment for the Energy Sector*, INFOSEC INSTITUTE (Aug 4, 2015), http://resources.infosecinstitute.com/cybersecurity-policy-and-threat-assessment-for-the-energy-sector/.

[xvi] *See* Igal Zeifman, *2015 Bot Traffic Report: Humans Take Back the Web; Bad Bots not Giving any Ground*, IMPERVA INCAPSULA (2015), https://www.incapsula.com/blog/bot-traffic-report-2015.html.

[xvii] *See* THREATTRACK, SECURITY ANALYSTS SAY DEFENDING AGAINST ADVANCED MALWARE STILL A MAJOR STRUGGLE (2016), *available at* http://land.threattracksecurity.com/Security-Analysts-Say-Defending-Against-Advanced-Malware-Still-A-Major-Struggle.html#_ga=1.48583078.1454101341.1479345130.

[xviii] ESET AND NATIONAL CYBERSECURITY ALLIANCE, BEHIND OUR DIGITAL DOORS: CYBERSECURITY & THE CONNECTED HOME 1 (2015), *available at* https://staysafeonline.org/download/datasets/19810/BEHIND%20OUR%20DIGITAL%20DOORS%20-%20ESET_NCSA%20Fast%20Facts.pdf.

[xix] ONLINE TRUST ALLIANCE, OTA FINDS 100% OF RECENTLY REPORTED IOT VULNERABILITIES EASILY AVOIDABLE (2016), *available at* https://otalliance.org/news-events/press-releases/ota-finds-100-recently-reported-iot-vulnerabilities-easily-avoidable.

[xx] *See HEWLETT PACKARD ENTERPRISE, MOBILE APPLICATION SECURITY REPORT 2016 (2016)* available at https://saas.hpe.com/sites/default/files/resources/files/Mobile%20Report%20ver%2010.2.pdf.

[xxi] *See*, *e.g.*, TYLER MOORE, INTRODUCING THE ECONOMICS OF CYBERSECURITY: PRINCIPLES AND POLICY OPTIONS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY. COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS NATIONAL RESEARCH COUNCIL (2010), *available at* http://www.nap.edu/read/12997/chapter/3.

[xxii] ADAM SMITH, THE WEALTH OF NATIONS 26 (1776).

[xxiii] *See* Federal Reserve Bank of St. Louis, The Role of Self-Interest and Competition in a Market Economy – The Economic Lowdown Podcast Series, Episode 3 (2015), https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-3-the-role-of-self-interest-and-competition-in-a-market-economy.

[xxiv] *See* Office of Management and Budget, Circular A-4, at 4 (Sept. 17, 2003) https://www.whitehouse.gov/omb/circulars_a004_a-4/.

[xxv] *See* Federal Reserve Bank of St. Louis, Externalities – The Economic Lowdown Podcast Series, Episode 11 (2015), https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-11-externalities.

[xxvi] *See* TYLER MOORE, INTRODUCING THE ECONOMICS OF CYBERSECURITY: PRINCIPLES AND POLICY OPTIONS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY. COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS NATIONAL RESEARCH COUNCIL (2010), *available at* http://www.nap.edu/read/12997/chapter/3.

[xxvii] *See* DOUGLAS LICHTMAN AND ERIC POSNER, HOLDING INTERNET SERVICE PROVIDERS ACCOUNTABLE, THE LAW AND ECONOMICS OF CYBERSECURITY 221-258 (eds. Mark F. Grady, F. Paris 2004), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=573502.

[xxviii] *See* ARTHUR C. PIGOU, THE ECONOMICS OF WELFARE (1920).

[xxix] *See* Robert D. Atkinson, *Framing a National Broadband Policy*, 16 COMMLAW CONSPECTUS 145, 145-164 (2007), *available at* http://commlaw.cua.edu/res/docs/07_Atkinson_145-177.pdf.

[xxx] *See* NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY, ESTIMATING USG IPv6 & DNSSEC EXTERNAL SERVICE DEPLOYMENT STATUS (2016), *available at* http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov.

[xxxi] *See* Sharon Goldberg, *Why Is It Taking So Long to Secure Internet Routing?* 12 ACMQUEUE 1 (2014), https://queue.acm.org/detail.cfm?id=2668966.

[xxxii] *See* Howard Kunreuther and Geoffrey Heal, *Interdependent Security*, 26 JOURNAL OF RISK AND UNCERTAINTY 231 (2003).

[xxxiii] *See id.*

[xxxiv] *See* VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT 15 (2015), *available at* http://www.verizonenterprise.com/DBIR/2015/.

[xxxv] *See* VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT 15 (2015), *available at* http://www.verizonenterprise.com/DBIR/2016/.

[xxxvi] *See* Press Release, Cloud Passage, CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education (April 7, 2016), https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/

[xxxvii] NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION, http://csrc.nist.gov/nice/about/index.html (last visited Sep. 26, 2016).

[xxxviii] NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, https://niccs.us-cert.gov/home/about-niccs (last visited Sep. 26, 2016).

[xxxix] *See id.*

[xl] *See* ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, GLOSSARY OF INDUSTRIAL ORGANISATION ECONOMICS AND COMPETITION LAW (1993), http://www.oecd.org/regreform/sectors/2376087.pdf.

[xli] *See* OECD Glossary of Statistical Terms, available at https://stats.oecd.org/glossary/detail.asp?ID=3256.

[xlii] *See* Policies Regarding Mobile Spectrum Holdings; Expanding Economic and Innovation Opportunities of Spectrum through Incentive Auctions, *Report and Order*, WT Docket Nos. 12-269, 12-268, 29 FCC Rcd 6133, 6135, 6211, paras. 4, 192-94 (2015).

[xliii] *See* FEDERAL COMMUNICATIONS COMMISSION, CELL PHONE UNLOCKING FAQS, https://www.fcc.gov/consumers/guides/cell-phone-unlocking-faqs (last visited Oct. 4, 2016).

[xliv] *See* WHITE HOUSE COUNCIL OF ECONOMIC ADVISERS ISSUE BRIEF, BENEFITS OF COMPETITION AND INDICATORS OF MARKET POWER 11-12 (April 2016), *available at* https://www.whitehouse.gov/sites/default/files/page/files/20160414_cea_competition_issue_brief.pdf.

[xlv] *See* Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act, *Broadband Progress Report*, GN Docket 15-191, 31 FCC Rcd 699, 736 (2016).

[xlvi] *See* ROSS ANDERSON, WHY INFORMATION SECURITY IS HARD – AN ECONOMIC PERSPECTIVE (ed. University of Cambridge Computer Laboratory, 2001), *available at* https://www.acsac.org/2001/papers/110.pdf.

[xlvii] *Id.*

[xlviii] *See* HENK KOX AND BAS STRAATHOF, ECONOMIC ASPECTS OF INTERNET SECURITY 18 (2013), http://www.cpb.nl/sites/default/files/publicaties/download/ad-kox-straathof-economic-aspects-internet-security.pdf.

[xlix] *See* FEDERAL COMMUNICATIONS COMMISSION, CONSUMER AFFAIRS AND OUTREACH DIVISION, https://www.fcc.gov/general/outreach (last visited Nov. 17, 2016).

[l] *See* FEDERAL COMMUNICATIONS COMMISSION, CYBERSECURITY FOR SMALL BUSINESS, https://www.fcc.gov/general/cybersecurity-small-business (last visited Nov. 17, 2016).

[li] *See* Wireless E911 Location Accuracy Requirements, *Fourth Report and Order*, PS Docket No. 07-114, 30 FCC Rcd 1259 (2015).

[lii] *See* KATIE DEY, SCIENCE OF CYBERSECURITY 4 (ed. JASON, 2010), http://cps-vo.org/node/2080.

[liii] *See* TYLER MOORE, INTRODUCING THE ECONOMICS OF CYBERSECURITY: PRINCIPLES AND POLICY OPTIONS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING

OPTIONS FOR U.S. POLICY. COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS NATIONAL RESEARCH COUNCIL 11 (2010), *available at* http://www.nap.edu/read/12997/chapter/3.

[liv] *See* HENK KOX AND BAS STRAATHOF, ECONOMIC ASPECTS OF INTERNET SECURITY 2 (2013), http://www.cpb.nl/sites/default/files/publicaties/download/ad-kox-straathof-economic-aspects-internet-security.pdf.

[lv] Department of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT) (2016), *available at* https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

[lvi] See Bruce Schneier, *Security Economics of the Internet of Things*, Schneier on Security (2016). https://www.schneier.com/blog/archives/2016/10/security_econom_1.html

[lvii] *See* Steve Morgan, *Top 5 Cybersecurity Facts, Figures and Statistics for 2017*, CSO (2016). http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html.

[lviii] *See* ROBERT H. SLOAN AND RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND SECURITY (2013).

[lix] *See* FRANK DICKSON, FROST & SULLIVAN, SECURE PIPES: CHANGING THE EXPECTATION OF YOUR INTERNET SERVICE PROVIDERS 3 (2015), *available at* http://www.level3.com/~/media/files/white-paper/en_dataserv_wp_fssecurepipes.pdf.

[lx] *See* MICROSOFT, RESPONSE TO THE DEPARTMENT OF COMMERCE GREEN PAPER ON CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY 18 (2011).

[lxi] *See* Final Report, U.S.Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs), Communications Security, Reliability and Interoperability Council III 2012 (March 2012), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[lxii] MUTUALLY AGREED NORMS FOR ROUTING SECURITY (MANRS), https://www.routingmanifesto.org/history/ (last visited Oct. 4, 2016).

[lxiii] *See id.*

[lxiv] *See id.*

[lxv] BRUCE BERKOWITZ AND ROBERT W. HAHN, CYBERSECURITY: WHO'S WATCHING THE STORE? (2003).

[lxvi] FRED H. CATE, ET AL., DOS AND DON'TS OF DATA BREACH AND INFORMATION SECURITY POLICY 6 (2009).

[lxvii] Treasury Department, Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636 6 (2013), *available at* https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf.

[lxviii] *See* Mike Sherling, *The Likely Regulators? An Analysis of FCC Jurisdiction over Cybersecurity*, 3 Federal Communications Law Journal 593 (2014).


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu