The Likely Regulators? An Analysis of FCC Jurisdiction over Cybersecurity

Mike Sherling*

TABLE OF CONTENTS

* J.D., *cum laude*, The George Washington University Law School, May 2014. The Author would like to thank Ethan Lucarelli and Charlie Pollack as well as the *FCLJ* members and editorial board for their valuable suggestions and feedback. The author would also like to thank his partner and his family for their support.

I. INTRODUCTION

In October 2012, Former Secretary of Defense Leon Panetta warned the nation of the potential for a "cyber Pearl Harbor" that would cause physical destruction and the loss of life.[1] "In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability," he stated gravely.[2] The attack could "be as destructive as the terrorist attack on 9/11."[3] While the Secretary's statements were arguably hyperbolic,[4] ineffective cybersecurity in the United States is a pressing problem, jeopardizing both national security and individual online safety.[5] Recent events clearly illustrate that cyber-attacks have become almost a daily part of life. Skilled attackers can use computer and network vulnerabilities to do everything from commit bank fraud to disrupt uranium enrichment.[6]

Part of the reason for this vulnerability to cyber-attacks is the lack of uniform implementation of existing, authoritative network security standards for Internet service providers ("ISPs"),[7] a problem that persists

---

1. Leon E. Panetta, Sec'y of Def., Dep't of Def., Speech before the Business Executives for National Security: Defending the Nation from Cyber Attack (Oct. 11, 2012), *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1728.

2. *Id.*

3. *Id.*

4. While hyperbolic, recent disclosures by Edward Snowden show the extent of United States cyber capabilities. These disclosures reveal wide-ranging abilities to infiltrate communications networks and platforms once thought secure. *See* Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923, 933–34 (2013); *see generally Edward Snowden*, THE GUARDIAN, http://www.theguardian.com/world/edward-snowden (last visited Dec. 25, 2013) (compiling articles on the NSA disclosures).

5. *See, e.g.*, Michael Riley, *Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-Internet-servers.html (detailing recent cyber-attacks).

6 *See generally* RYAN SHERSTOBITOFF, ANALYZING PROJECT BLITZKRIEG, A CREDIBLE THREAT, MCAFEE (Dec. 2012), *available at* http://www.mcafee.com/us/resources/white-papers/wp-analyzing-project-blitzkrieg.pdf; NICOLAS FALLIERE, LIAM MURCHU & ERIC CHIEN, W32.STUXNET DOSSIER, SYMANTEC (Feb. 2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; Jim Finkle & Dhanya Skariachan, *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, REUTERS (Dec. 19, 2013), http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219.

7. *See, e.g.*, *DNS-based Authentication of Named Entities*, IETF (2012), https://datatracker.ietf.org/wg/dane/. The Internet Engineering Task Force ("IETF") is an international community of network designers, operators, vendors, and researchers with the goal of creating specifications of high technical quality while considering the interests of all of the affected parties and while establishing widespread community consensus. *See IETF Standards Process*, IETF (2012), http://www.ietf.org/about/standards-process.html. Throughout this Note, the terms "minimum cybersecurity standards," "minimum standards," and "industry best practices" are used interchangeably. *See 911 Reliability Order*, *infra* note 192, at para. 46 (noting that "best practices are developed in a 'consensus-based

because ISPs are under no obligation to implement these standards.[8] Together, these factors have created a market that often fails to provide adequate cybersecurity.[9]

When a market fails to provide a necessary service, such as the guaranteed integrity of the communications network, the government can step in to fill the gap. This Note argues that the Federal Communications Commission ("FCC") has the authority to require ISPs to implement network level cybersecurity measures to maintain the integrity and security of the networks. The FCC derives this power from its ancillary authority in Title I of the Communications Act of 1934 and its statutory mandates to ensure a reliable communications network and implement 9-1-1 service over VoIP.[10]

To establish the FCC's authority in this area, this Note examines some of the causes of and partial solutions to cyber-attacks in relation to FCC authority. Part II gives background on network security and cyber-attacks, and details the FCC's ancillary authority, which allows the FCC to promulgate regulations concerning technology over which it does not have a direct statutory mandate. Part III analyzes the FCC's ability to use its ancillary authority to require ISPs to implement cybersecurity standards, concluding that the FCC has jurisdiction to implement minimum standards because insufficient cybersecurity could catastrophically impact services the FCC oversees. Part IV considers whether the FCC should exercise its ancillary authority, determining that the market failure in cybersecurity vulnerability information and network reliability, together with the compelling need for a reliable communications system, justifies

---

environment' reflecting the collective judgment of industry, government, and other stakeholders.").

8. *See* Austin Schlick, FCC General Counsel, FCC, *A Third-Way Legal Framework for Addressing the* Comcast *Dilemma* (May 6, 2010), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-297945A1.pdf (noting "the Commission's settled, deregulatory policy framework for broadband communications services.").

9. *See, e.g.*, ATLANTIC COUNCIL, A FIERCE DOMAIN: CONFLICT IN CYBERSPACE 13 (Jason Healey ed., forthcoming 2013) (on file with editor) ("We've had market failure when it comes to cybersecurity. Security doesn't come out of voluntary actions and market forces.") (quoting Deputy Secretary of Defense Ashton Carter at the RSA Conference in 2012); *see also id.* ("The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.") (quoting National Academy of Science report, Computers at Risk in 1991); Christian F. Binnig, *The Legal and Policy Challenges of a Rapidly Changing Telecommunications Industry*, *in* RECENT DEVELOPMENTS IN TELECOMMUNICATIONS LAW 9 (Oct. 2013), *available at* 2013 WL 6117748; *cf.* Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting, *Notice of Proposed Rulemaking*, FCC 11-74, para. 20 (2011) [hereinafter VoIP Outage Reporting NPRM] ("The economic justification to ensure [Internet] service appears to be limited, and does not consider network externalities. Moreover, even if incentives did motivate individual market participants to optimize their own reliability, they do not necessarily optimize systemic reliability.") (citations omitted).

10. *See* 47 U.S.C. § 615a-1 (2006); Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended at scattered sections 47 U.S.C.).

government regulation. The Note concludes with a brief discussion of the costs and benefits of potential regulation.

II. BACKGROUND

The near consensus is that the current state of cybersecurity is abysmal.[11] For example, the computer security firm McAfee has over 100 million samples of malware in its database.[12] The National Vulnerability Database contains over 50,000 software vulnerabilities that malicious actors can exploit;[13] myriad industries experience cyber-attacks daily.[14] The magnitude of the problem is staggering.

With threats coming from all over the world this is both a national and international problem.[15] In 2005, American corporations lost an estimated $867 million due to cyber-attacks, cyber theft, and other computer security incidents.[16] Recent high-profile events include attacks against the security firm RSA,[17] Google,[18] the financial sector,[19] oil companies,[20] and several others.[21] Moreover, it is more than just corporate

---

11. Jason Ryan, *NSA Director on Cyberattacks: 'Everybody's Getting Hit'*, ABC NEWS (Nov. 7, 2012), http://abcnews.go.com/blogs/politics/2012/11/nsa-director-on-cyberattacks-everybodys-getting-hit (cataloging a myriad range of companies hit by cyber-attacks in 2011). *But see* Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT. SEC. J. 39 (2011) (desiring a more thorough justification to buttress calls for increased resources to be devoted to cyber-threats), *available at* http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.

12. MCAFEE LABS, *McAfee Threats Report: Third Quarter* 2012, at 9, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf (last visited Nov. 15, 2012).

13. NATIONAL VULNERABILITY DATABASE, http://nvd.nist.gov (last visited Nov. 17, 2012). As of November 17, 2012, the database contained 53,914 common vulnerabilities and exposures. *Id.*

14. MCAFEE LABS, *supra* note 12, at 23–24.

15. *See, e.g.*, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, MANDIANT 22 (2013) [hereinafter MANDIANT REPORT], *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (noting attacks originating from China against 15 different countries).

16. RAMONA R. RANTALA, DEP'T OF JUSTICE, *Cybercrime Against Businesses*, at 1 (Sept. 2008), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf. Other computer security incidents include attacks using spyware, ad-ware, hacking, phishing, spoofing, pinging, port scanning regardless of whether the attack was successful. *Id.* at 2.

17. *See generally* Zeljka Zorz, *RSA Hacked, SecurID Users Possibly Affected*, HELP NET SEC. (Mar. 18, 2011), http://www.net-security.org/secworld.php?id=10763.

18. Kevin P. Newmeyer, *Cyber Espionage: A Threat to National Security*, 10 SEC. & DEF. STUD. REV., Spring-Summer 2010, at 116.

19. *See* MCAFEE LABS, *supra* note 12, at 7.

20. *See, e.g.*, Michael Riley, *Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-Internet -servers.html.

21. *See* Ryan, *supra* note 11.

networks that are under attack; cyber-attacks also compromise the basic computer infrastructure of the Internet.

A. Network Security Standards and Cyber-attacks

Uniform implementation of industry-developed network security standards by ISPs could significantly reduce overall vulnerability to cyber-attacks. For example, one of the foundational elements of the Internet, the Domain Name System ("DNS"), has well-known flaws.[22] The DNS is a set of computers that translates user-friendly text, such as website addresses, into the string of numbers (Internet Protocol, or IP, addresses)[23] that computers use to communicate on the Internet.[24] In the Internet's nascent days, the engineers who created the Internet chose a standard that did not emphasize security, instead focusing on ease of integration and interoperability.[25] As a result, the DNS is vulnerable to attacks By malicious actors who can hijack and reroute Internet traffic from the intended website to their own server.[26] In a case involving bank fraud, for example, when a person tries to access an online banking website, her computer connects to a DNS server on the Internet and receives the IP address of the bank website.[27] However, if a cyber-attacker provides the DNS server with the wrong IP address, the server would direct her browser to a malicious website that can capture bank login information.[28]

In the mid-1990s, as the vulnerabilities of DNS became apparent, the development of a more secure system—known as Domain Name System Security Extensions ("DNSSEC")—began in earnest. DNSSEC was finalized in 2005, and by 2010, major Internet authorities, such as the Internet Corporation for Assigned Names and Numbers ("ICANN") and

---

22. *See* JOHN KRISTOFF & RODNEY JOFFEE, NEUSTAR ULTRA SERVICES, *Botnets and Packet Flooding DDoS Attacks on the Domain Name System* 1 (2007), *available at* http://layer9.com/~jtk/papers/dnsddos.pdf; *see generally DNS Threats & Weaknesses of the Domain Name System*, DNSSEC: DNS SECURITY EXTENSIONS, http://www.dnssec.net/dns-threats.php (last visited Nov. 15, 2012).

23. This Note uses the term IP or Internet Protocol as shorthand for the TCP/IP Suite and related technologies that mediate the packet-switched communications. For an in-depth discussion of the technology that powers the internet and modern communications networks, see Douglas C. Sicker & Lisa Blumensaadt, *Misunderstanding the Layered Model(s)*, 4 J. TELECOMM. & HIGH TECH. L. 299 (2006) and Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707 (2013).

24. CSRIC III WORKING GROUP 5, *DNSSEC Implementation Practices for ISPs*, at 10 (2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf.

25. *See* PAUL MOCKAPETRIS, INFORMATION SCIENCES INSTITUTE, *Domain Names - Concepts and Facilities*, at 2–3 (1987), *available at* http://tools.ietf.org/html/rfc1034 (discussing purposes of the Domain Name System).

26. *DNSSEC Implementation Practices for ISPs*, *supra* note 24, at 17.

27. *See id.* at 10.

28. *See id.* at 17.

VeriSign, had upgraded to DNSSEC.[29] In domain name resolution, distinct roles are performed by root servers, ISP DNS servers, and Internet domains. A critical mass of all three types of operators is necessary for DNSSEC to function as intended. So far, only the root servers, some ISPs, and government servers have implemented DNSSEC, as there is no requirement to adopt it.[30] As of 2013, only Comcast has deployed DNSSEC in its subsidiary DNS servers,[31] and a paltry two percent of non-government domains run DNSSEC in the United States, reflecting the lack of incentive to do so.[32]

Another security standard that, if uniformly implemented, would strengthen the resiliency of the Internet is the Secure Border Gate Protocol ("BGP").[33] The insecure nature of the current BGP standard creates opportunities for malicious action by misconfiguring one BGP router to send out false information so as to capture or reroute private traffic as it travels over the Internet to a targeted server or group of IP addresses.[34] Other BGP routers will utilize that information to send traffic to the erroneous address.[35] The world saw this firsthand when Pakistan famously "took down YouTube" by configuring its BGP router to broadcast that it had the YouTube IP addresses within its network.[36] That information spread to other BGP routers, who started sending traffic intended for

29. Press Release, Dep't of Commerce, ICANN and VeriSign Deploy New Technology to Enhance the Security and Stability of the Internet (Jul. 16, 2010), *available at* http://www.commerce.gov/news/press-releases/2010/07/16/commerce-department-icann-and-verisign-deploy-new-technology-enhance-.

30. *DNSSEC Implementation Practices for ISPs*, *supra* note 24, at 17.

31. Jason Livingood, *Comcast Completes DNSSEC Deployment*, COMCAST VOICES (Jan. 10, 2012), http://blog.comcast.com/2012/01/comcast-completes-dnssec-deployment.html.

32. *Estimating IPv6 & DNSSEC Deployment Status*, NAT'L INST. OF STANDS. & TECH., http://usgv6-deploymon.antd.nist.gov/snap-all.html (last visited Nov. 17, 2012) (showing 2% of domains have DNSSEC operational, 1% are in progress, and 98% have no progress).

33. BGP is one way that servers route Internet packets through the network. CSRIC III WORKING GROUP 6, *Secure BGP Deployment*, 12 (2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Final-Report.pdf. By way of background, the Internet is a set of interconnected networks. Each major service provider has its own self-contained network, called an Autonomous System, which is a collection of IP addresses that all connect to the rest of the Internet through the service provider's "gates." *Id.* The ISP uses the Border Gate Protocol to control how traffic moves into and out of its network. *Id.* Each ISP chooses how its BGP routes traffic to its internal network according to a multitude of considerations, such as business relationships and the other Autonomous Networks to which the ISP connects. *Id.* Because of the great power these servers have in controlling Internet traffic, each ISP relies on and trusts each other ISP to implement their BGP routing policy in a truthful way, i.e. in a way that reasonably passes along traffic that does not terminate within its network. *Id.* This trust manifests in the fact that BGP routers blindly accept information from other BGP routers about what is on their networks. *Id.*

34. *Id.*

35. *Id*. at 12.

36. Martin A. Brown, *Pakistan Hijacks YouTube*, RENESYS (Feb. 24, 2008), http://www.renesys.com/blog/2008/02/pakistan-hijacks-youtube-1.

YouTube to Pakistan's servers.[37] Internet operators can remedy this misinformation relatively quickly; for example, in this case, network operators isolated Pakistan and fixed the routing tables within two hours.[38] A standard that cryptographically secures the designated path so malicious routers cannot alter the path of specific traffic within the packet could prevent this from happening again in the future.[39]

The examples above are just two of the innumerable security vulnerabilities that exist. To stem the abuse of these vulnerabilities, the National Institute of Standards and Technology recently developed a Cybersecurity Framework to help organizations secure critical infrastructure.[40] Implementing some of these suggestions could fix a portion of the security problems facing ISPs.[41]

These and other vulnerabilities have never been more important given the impending transition of our communications networks from the circuit-based Public Switched Telephone Network ("PSTN") to a flexible, all-IP network over which voice, video, and Internet traffic flow.[42] After this transition, communications that were once transmitted through separate networks, such as telephone and cable networks, will be transmitted through the Internet or using Internet Protocol, both of which are far more susceptible to cyber-attacks than the PSTN.[43] In contrast to the separate communications networks of the twentieth century, when there were only a small number of notable broadcast signal intrusion events and

---

37. *Id.*

38. *Id.*

39. *Id.*

40. *See* FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *infra* note 66.

41. *Id.*

42. *See* AT&T, Petition to Launch a Proceeding Concerning the TDM-to-IP Transition at 2, FCC GN Docket No. 12-353 (rel. Dec. 18, 2012) [hereinafter AT&T IP Transition Petition], *available at* http://apps.fcc.gov/ecfs/document/view?id=7022086087 (quoting Connect America Fund, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 11-161, 26 FCC Rcd. 17663, 17926 (2011)) (asking the FCC to "take the next steps to 'facilitate the transition' away from the legacy TDM-based network to an 'all-IP network' that is capable of supporting broadband Internet access, higher-layer VoIP, and other advanced communications services"); *see also* FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN § 4.5 (2010), *available at* http://download.broadband.gov/plan/national-broadband-plan.pdf.

43. *See* Initial Comments of the National Association of State Utility Consumer Advocates at 18, AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition, FCC GN Docket No. 12-353 (rel. Jan. 28, 2013), *available at* http://apps.fcc.gov/ecfs/document/view?id=7022113102 (stating concerns about cybersecurity as a result of the transition); Reply Comments of the Computer & Communications Industry Association (CCIA) at 13, AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition, FCC GN Docket No. 12-353 (rel. Feb. 25, 2013), *available at* http://www.ccianet.org/wp-content/uploads/library/FCC%20Comments%20on%20Transition_to_IP_Networks.pdf (requesting that the FCC consider cybersecurity when proposing regulations on the transition).

communication disruptions,[44] the Internet has made it possible to communicate—or, in some cases, alter others' communications—throughout the world. This is a double-edged sword, as interconnection is essential in a networked world.[45] Governments recognize this and hack administrators of telecommunications networks to intercept the communications on those networks; while this has been used for surveillance, it could be also be used to disrupt communications.[46]

The Internet is built on the idea that packets may take many different paths to get from their source to their destination.[47] But this interconnectedness is also what makes the network vulnerable to cyber-attacks, as a failure or error in one system can propagate through the network.[48] Today, websites are routinely defaced, denial of service attacks prevent people from accessing the Internet,[49] and, significantly, it is easy to commandeer the Emergency Alert System.[50] Even though the distributed nature of the network provides some internal resilience, that resilience can be strained. If many networks or connections between networks are brought down in a cyber-attack, the remaining nodes on the Internet will have fewer routing options, which could cause a bottleneck that slows communications down or stops them completely.[51] Finally, if the routers and servers use the

---

44. *See, e.g.*, Alan Bellows, *Remember, Remember the 22nd of November*, DAMN INTERESTING (Jan. 9, 2007), http://www.damninteresting.com/?p=776 (detailing the Max Headroom broadcast signal intrusion event in Chicago on November 22, 1987 where an unknown person hijacked the signal of WGN-TV and WTTW to broadcast an impersonation of the character Max Headroom). The Max Headroom broadcast signal intrusion event is available on YouTube at http://www.youtube.com/watch?v=h5mzkt4N77s.

45. 47 U.S.C. § 251(a)(1); Kevin Werbach, *Off the Hook*, 95 CORNELL L. REV. 535, 588 (2010).

46. *Cf.* Ryan Gallagher & Peter Maass, *Inside the NSA's Secret Efforts to Hunt and Hack System Administrators*, THE INTERCEPT (Mar. 20, 2014), https://firstlook.org/theintercept/article/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/ (detailing NSA efforts to hack system administrators to gain access to the networks they administer). Indeed, the NSA disclosures show that the U.S. government has the ability to prevent a user from reaching websites. *See* THERE IS MORE THAN ONE WAY TO QUANTUM, NAT'L SEC. ADMIN., *available at* https://firstlook.org/theintercept/document/2014/03/12/one-way-quantum/ (describing QUANTUMSKY, an NSA technique that denies access to a webpage through RST packet spoofing).

47. *Id.*

48. *See* Brown, *supra* note 36 (describing the propagation of Pakistan's BGP problem); Randy Picker, *Cybersecurity: Of Heterogeneity and Autarky*, *in* THE LAW & ECONOMICS OF CYBERSECURITY 115, 124 (Mark F. Grady & Francesco Parisi eds., 2005).

49. Jeffrey L. Goldings, *Hackers Leave Their Mark on Websites*, 2 No. 8 QUINLAN, COMPUTER CRIME & TECH. IN LAW ENFORCEMENT art. 13, Aug. 2006.

50. *See Zombies? Emergency Broadcast System Hacked*, UPPERMICHIGANSSOURCE.COM, WLUC TV6 (Feb. 12, 2013), http://www.uppermichiganssource.com/news/story.aspx?id=859352#.

51. *See, e.g.*, Michael Lee, *The Largest DDoS Attack Didn't Break the Internet, but It Did Try*, ZDNET (Mar. 28, 2013), http://www.zdnet.com/the-largest-ddos-attack-didnt-break-the-internet-but-it-did-try-7000013225/ (discussing slow Internet speeds in Europe as a result of a recent cyber-attack).

same insecure standards, attacks can propagate through the whole network. This is the lens through which one must view FCC authority.

B. The FCC's Historical Role in Cybersecurity

The FCC has previously attempted to improve cybersecurity and the security of the communications grid. In these attempts, the FCC has expressed skepticism about whether market forces adequately incentivize ISPs to implement "measures to maintain the high-quality security, reliability and resiliency of their respective services."[52] Because the FCC has expertise in communications issues, other federal agencies expect it to comment on cybersecurity policy; this is evidenced by the FCC's substantial contribution to the White House 60-Day Cyberspace Policy Review.[53]

In the National Broadband Plan, the FCC discussed the need for improved cybersecurity in the telecommunications sector and potential methods of implementation.[54] Perhaps the most comprehensive and important work that the FCC has produced on cybersecurity has been through federal advisory committees.[55] In most circumstances, a federal advisory committee has solely an advisory role, with its recommendations not carrying the force of law.[56] One such committee was the Network Reliability and Infrastructure Council ("NRIC"). It developed a number of cybersecurity best practices and made a recommendation that private industry voluntarily implement these best practices.[57]

The successor to NRIC, is the Communications Security, Reliability and Interoperability Council ("CSRIC"). It focuses on strengthening cybersecurity, ensuring availability of communications networks during an emergency or disaster, and developing procedures that communications providers can take to improve cybersecurity.[58] CSRIC has made significant recommendations on ways to improve cybersecurity at the network level.

---

52. *See* VoIP Outage Reporting NPRM, *supra* note 9, at para. 20.

53. Cyber Sec. Certification Program, *Notice of Inquiry*, FCC 10-63, para. 5, (2010) [hereinafter Cyber Sec. Certification Program NOI], *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-10-63A1.pdf; WHITE HOUSE, CYBERSPACE POLICY REVIEW, at 4 (2009) [hereinafter CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (discussing U.S. Government cybersecurity initiatives).

54. *See National Broadband Plan*, supra note 42, § 16.2.

55. A federal agency can convene advisory committees that consist of private sector experts for the purpose of advising the agency. *See* 5 U.S.C. app. 2 § 2 (2006).

56. *See id.* at § 2(b). This is the case for the FCC advisory committees discussed here.

57. *See* Cyber Sec. Certification Program NOI, *supra* note 53, at paras. 6-7.

58. *See Charter of Network Reliability and Interoperability Council* at 1, *available at* http://transition.fcc.gov/hspc/NRIC_recharter.pdf (last accessed on Nov. 15, 2012); *Charter of the FCC's Communications Security, Reliability, and Interoperability Council*, at 1 [hereinafter *CSRIC Charter*], *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC%20Charter%20Renewal%202011%20FINAL.pdf (last accessed on Nov. 15, 2012).

Like NRIC, however, the Council is purely advisory, so it lacks the authority to require the FCC or private industry to follow its recommendations.[59]

CSRIC III [60] issued recommendations for voluntary industry guidelines to combat three major cybersecurity threats, including botnets, attacks on the Domain Name System, and Internet route hijacking through the use of the insecure Border Gate Protocol. [61] These security vulnerabilities are particularly important, as attacks on these systems could cause widespread access problems for certain parts of the Internet.[62]

However, CSRIC's guidelines are voluntary, so the major ISPs pledging to implement them serve only fifty percent of residential broadband users. [63] There are currently no mandatory cybersecurity standards for our nation's private telecommunications networks.

One promising recent development is an Executive Order entitled *Improving Critical Infrastructure Cybersecurity*.[64] It mandated that the National Institute of Standards and Technology and the Department of Homeland Security ("DHS") create a set of standards and procedures that align policy, business, and technological approaches to address cyber-threats to all sectors of the nation's critical infrastructure, including the nation-wide communications infrastructure.[65] NIST released Cybersecurity Framework Version 1.0 on February 12, 2014.[66] As a methodology, the Framework does not require organizations to implement specific standards to improve cybersecurity.[67] Instead, NIST suggests that organizations use

---

59. *See* 5 U.S.C. app. 2 § 2; *CSRIC Charter*, *supra* note 58, at 1.

60. CSRIC III is the third authorization of the federal advisory committee.

61. Press Release, FCC, FCC Advisory Committee Adopts Recommendations to Minimize Three Major Cyber Threats, 2012 WL 983082, at *2 (Mar. 22, 2012), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-313158A1.pdf.

62. I do not discuss the Anti-Botnet Code of Conduct. Botnets can perform distributed denial of service attacks on a website or computer connected to the Internet. However, the solutions proposed by CSRIC III to combat botnets are not technical, but instead rely on user education and notification, and as such do not lend themselves to standardization. *See* CSRIC III WORKING GROUP 7, *Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, at 3 (Mar. 2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf; *see also* T. Luis de Guzman, Comment, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 528–29 (2010).

63. CSRIC Press Release, *supra* note 61, at *2.

64. *Improving Critical Infrastructure Cybersecurity*, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) [hereinafter Cybersecurity Executive Order].

65. *Id.* at 11,741.

66. FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.0, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, February 12, 2014, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

67. The Framework does contain "Informative References," which are "specific sections of standards, guidelines, and practices common among critical infrastructure sectors

the Framework to identify opportunities to strengthen and communicate their management of cybersecurity risk while aligning with industry practices.[68]

The most recent incarnation of the Communications Security, Reliability, and Interoperability Council, CSRIC IV, is currently working to evaluate CSRIC's most critical existing cybersecurity best practices and determine how best to improve them to account for changes in cybersecurity practice and the threat landscape.[69] It will then harmonize and update these best practices with the NIST Cybersecurity Framework.[70] However, as noted above and discussed in detail in Part VI below, firms currently have no incentive other than market pressure to upgrade the cybersecurity of the Internet. Even with the NIST Cybersecurity Framework and CSRIC's best practices as guides, mandating that ISPs implement them would bring the FCC into new territory, as the Internet is outside of the FCC's traditional regulatory role.

C. The FCC's Jurisdiction over the Internet

The FCC's power to regulate communications activities is quite broad. For example, Title I of the Communications Act of 1934 gives the FCC jurisdiction over "all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio."[71] The 1934 Act enumerates specific responsibilities and powers with respect to common carriers and wire communication (Title II)[72] and radio wave transmissions (Title III);[73] Congress gave the FCC jurisdiction over cable service in 1984 (Title VI).[74]

These statutes mandate FCC oversight and promotion of specific communications services. For example, the FCC oversees common carriers,[75] ensures interconnection between telecommunications carriers,[76] promulgates rules to ensure 9-1-1 service,[77] and promotes diversity of

---

that illustrate a method to achieve" certain security outcomes. However, these are illustrative and not exhaustive. *See id.* at 8.

68. *Id.* at 4.

69. CSRIC IV - Working Group 4: Cybersecurity Best Practices Status Update, March 20, 2014 at 5, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_WG4_STATUS_03202014.pdf.

70. *Id.*

71. Communications Act of 1934, ch. 652, § 2, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 152(a) (2006)).

72. *Id.* § 201 (codified as amended at 47 U.S.C. § 201 (2006)).

73. *Id.* § 301 (codified as amended at 47 U.S.C. § 301 (2006)).

74. Cable Communications Policy Act of 1984, Pub. L. No. 98–549, 98 Stat. 2779 (1984) (codified at scattered sections 47 U.S.C.). This statute was enacted after the FCC successfully asserted its jurisdiction over cable services in the 1960s. *See* United States v. Southwestern Cable Co., 392 U.S. 157 (1968), *infra* note 99 and accompanying text.

75. *See* 47 U.S.C. §§ 201-231 (2006).

76. *See* 47 U.S.C. § 251 (2006).

77. 47 U.S.C. § 615a-1 (2006).

information sources and services provided in cable communications.[78] Furthermore, the FCC's general purpose is to regulate "interstate and foreign commerce in communication by wire and radio so as to make available . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense [and] promoting safety of life and property."[79] However, the FCC's enabling statutes do not confer upon it direct authority over the Internet.[80]

The character of the regulation the FCC can promulgate depends heavily on the type of service regulated, as evidenced by the demarcation between the different titles of the FCC's enabling statutes. One of the FCC's primary areas of authority throughout the twentieth century was the regulation of the Public Switched Telephone Network ("PSTN"), which AT&T provided as a common carrier.[81] In the 1970s, "enhanced" services such as data transmission became available.[82] The FCC did not have direct authority over enhanced services, as they differed from basic telephone service.[83] The statutory distinction between "telecommunications service" and "information service" reflects the historical distinction between basic and enhanced services, and maintains the practice restricting FCC direct authority to telecommunications services.[84]

The Telecommunications Act of 1996 defines a telecommunications service as the "offering of telecommunications for a fee directly to the public . . . regardless of the facilities used."[85] The FCC must treat telecommunications carriers as common carriers "only to the extent that [they] . . . engage[] in providing telecommunications services."[86] In contrast, an information service is one that offers the "capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and

78. *See* 47 U.S.C. § 521 (2006) (FCC mandated to assure that cable communications provide and are encouraged to provide the widest possible diversity of information sources and services to the public).

79. 47 U.S.C. § 151 (2006).

80. *But see* 47 U.S.C. § 230(b) (stating broad policy statements about the Internet and immunizing ISPs from liability for content they did not create); 47 U.S.C. § 1302(b) (requiring the FCC to promote broadband deployment under certain circumstances).

81. *See* United States v. AT&T, 552 F. Supp. 131, 178 (D.D.C. 1982), *aff'd sub nom.,* Maryland v. United States, 460 U.S. 1001 (1983) (discussing AT&T's business in the last half of the twentieth century).

82. *See* Computer & Commc'ns Indus. Ass'n v. FCC, 693 F.2d 198, 203–06 (D.C. Cir. 1982) (*CCIA v. FCC*).

83. *Id.* at 207.

84. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 996 (2005).

85. Telecommunications Act of 1996, Pub. L. No. 104-104, § 101(a), 110 Stat. 56 (1996) (codified at 47 U.S.C. § 153(53) (2006)).

86. *Id.* § 3 (codified at 47 U.S.C. § 153(51) (2006)). The FCC wields substantial authority over the practices of telecommunications carriers because they are regulated as common carriers. *See generally* 47 U.S.C. §§ 201-231.

includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service."[87] There are no corresponding common carriage or regulatory requirements for information services.[88]

In a series of rulemakings conducted in the early 2000s, the FCC classified broadband services as information services, thereby precluding the agency from regulating broadband service as a common carrier.[89] The information service classification includes cable broadband service,[90] wireless broadband service,[91] wireline broadband service,[92] and broadband service over power lines.[93] The FCC makes a delicate distinction between the services that an ISP provides, ultimately concluding that ISPs provide a connection to the Internet "via telecommunications."[94] This formulation indicates that the FCC cannot use its traditional Title II regulatory tools to regulate broadband.[95]

D. The FCC's Ancillary Authority

Because broadband ISPs provide information services, the FCC's ability to place regulatory obligations on ISPs is limited. The FCC can regulate an information service, however, if the information service impacts another service the FCC is empowered to regulate by statute. This is known as the FCC's ancillary authority.[96] The Communications Act of 1934 authorized the FCC to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as

87. Communications Act of 1934, ch. 652, § 153(20), 48 Stat. 1064 (codified as amended at 47 U.S.C. § 153(24) (2006)).

88. *See* Verizon v. FCC, 740 F.3d 623, 649–51 (D.C. Cir. 2014).

89. *Id*.

90. Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 986–87 (2005); *see generally* High-Speed Access to the Internet Over Cable and Other Facilities, *Declaratory Ruling and Notice of Proposed Rulemaking*, FCC 02-77 (2002) [hereinafter Cable Broadband Ruling].

91. Appropriate Regulatory Treatment for Broadband Access to the Internet over Wireless Networks, *Declaratory Ruling*, FCC 07-30, paras. 22, 29 (2007) [hereinafter Wireless Broadband Ruling].

92. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, FCC 05-150, paras. 15, 103–04 (2005) [hereinafter Wireline Broadband Report and Order], *aff'd sub nom.,* Time Warner Telecom, Inc. v. FCC, 507 F.3d 205 (3d Cir. 2007).

93. Classification of Broadband over Power Line Internet Access Service as an Information Service, *Memorandum Opinion and Order*, FCC 06-165, paras. 9, 12 (2006).

94. Cable Broadband Ruling, *supra* note 90, at para. 41. This distinction contrasts with another possible interpretation, that broadband service itself is actually providing telecommunications.

95. *See* 47 U.S.C. §153(20); Verizon v. FCC, 740 F.3d 623, 649–51 (D.C. Cir. 2014).

96. *See* Comcast Corp. v. FCC, 600 F.3d 642, 646–47 (D.C. Cir. 2010); *see generally id.* (giving a summary of the early Supreme Court ancillary authority rulings).

may be necessary in the execution of its functions."[97] The Supreme Court has interpreted this authority to allow the FCC to take actions that further its statutory mandate, even if not expressly contemplated by a statute.[98] The purpose of this penumbra of authority surrounding the FCC's statutorily conferred power is to allow the FCC to adapt government telecommunications policy to new technology in a more efficient and flexible way than Congress could.[99]

Ancillary authority has been used most prominently to regulate communications services over which the FCC does not have an explicit grant of authority, but that nevertheless affect services that the FCC regulates. The Court's treatment of cable television in *United States v. Southwestern Cable Co.*[100] provides an example of the FCC's lawful regulation of a technology that did not exist when the Communications Act of 1934 was enacted, but that had the potential to disrupt the broadcast television market—over which the FCC has a mandate.[101] The Court stated that the characteristics of the new service are relevant only to determine whether it satisfies the FCC's general jurisdictional grant, which includes interstate communication by radio or wire, as a prerequisite to jurisdiction.[102] After this threshold is satisfied, a reviewing court then looks to the impact the new service has on existing regulated services.[103] If the new service could prevent the FCC from achieving statutory goals associated with the established service, then a court looks to how the proposed regulation fits into the Commission's current rules.[104]

The D.C. Circuit, in *American Library Association v. FCC*,[105] issued the pronouncement on FCC ancillary authority that governs to this day.[106] To use its ancillary authority as a basis for a regulation, the FCC must satisfy two requirements. First, the FCC's "general jurisdictional grant" under Title I must cover the regulated subject.[107] Second, the regulations must be reasonably ancillary to the FCC's effective performance of its statutorily mandated responsibilities.[108]

---

97. Communications Act of 1934, ch. 652, § 4(i), 48 Stat. 1066 (codified at 47 U.S.C. § 154(i) (2006)).

98. United States v. Midwest Video Corp. (*Midwest I*) 406 U.S. 649, 669-70 (1972) (plurality opinion).

99. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 172 (1968) (quoting FCC v. Pottsville Broad. Co., 309 U.S. 134, 138 (1940)).

100. *See id.* at 172.

101. *Id.*

102. *See Midwest I*, 406 U.S. at 659-60; *see also* Werbach, *supra* note 45, at 580.

103. *See Southwestern Cable*, 392 U.S. at 174–78.

104. *See id.* at 178-79; *see also* Werbach, *supra* note 102, at 580.

105. Am. Library Ass'n v. FCC, 406 F.3d 689, 691-92 (D.C. Cir. 2005).

106. *Id.*

107. *Id.*

108. *Id.* Stated another way, the regulation at issue should be "imperative if [the FCC] is to perform with appropriate effectiveness . . . its other responsibilities." *Southwestern Cable*, 392 U.S. at 173.

Regarding the first requirement, the FCC's general jurisdictional grant is broad, encompassing authority over "all interstate and foreign communication by wire or radio." [109] Even where a communication emanates from and is received within the same state, it falls within the reach of Title I insofar as it is part of a broader national network. [110] Accordingly, the FCC's Title I general jurisdiction likely includes the provision of communications services over the Internet such as broadband Internet access.[111]

The second requirement, that the regulations must be reasonably ancillary to the FCC's effective performance of its statutorily mandated responsibilities, is more difficult to satisfy. A court evaluates the permissibility of each new exercise of ancillary authority on its own terms.[112] That is, the FCC cannot justify a new use of ancillary authority by reference to previous incarnations of this authority.[113]

For example, in the seminal ancillary authority case, *Southwestern Cable*, the Supreme Court analyzed the FCC regulations over community antenna television ("CATV"), a service known today as cable television.[114] When the Court heard the case in 1968, Congress had not afforded the FCC express authority over CATV, but Congress had mandated that the Commission ensure "a widely dispersed radio and television service, with a fair, efficient, and equitable distribution of service among the several States and communities."[115] The FCC reasonably concluded that CATV could "'destroy or seriously degrade the service offered by a television broadcaster, and thus ultimately deprive the public of the various benefits of a system of local broadcasting stations."[116] Accordingly, because CATV posed a threat to a service that Congress required the FCC to keep operational, the FCC's exercise of its ancillary authority to promulgate CATV regulations was upheld as valid.

---

109. *See* 47 U.S.C. § 152 (2006).

110. *See Southwestern Cable*, 392 U.S. at 168–69 (stating that intrastate broadcasting and cablecasting still fall within the FCC's Title I authority because they consist of programming devised for and distributed to a national audience).

111. That neither the FCC nor Comcast disputed the validity of broadband falling with the Commission's Title I grant tilts heavily toward this conclusion. However, because the court reversed the FCC on other grounds, this issue has not been conclusively decided. *See Comcast*, 600 F.3d at 646–47 (stating that "Comcast concedes that the Commission's action here [regulating broadband Internet] satisfies the first requirement because the company's Internet service qualifies as 'interstate and foreign communication by wire' within the meaning of Title I of the Communications Act") (citation omitted).

112. *Id.* at 650; *see Midwest Video I*, 406 U.S. at 669–70 (plurality opinion).

113. Comcast Corp. v. FCC, 600 F.3d 642, 650 (D.C. Cir. 2010).

114. *Evolution of Cable Television*, FCC ENCYCLOPEDIA (2012), http://www.fcc.gov/encyclopedia/evolution-cable-television.

115. *Southwestern Cable*, 392 U.S. at 174–76 (internal quotation marks and citations omitted); *see* 47 U.S.C. § 307(b).

116. *Southwestern Cable*, 395 U.S. at 175–76 (quoting Grant of Authorizations in the Bus. Radio Serv. for Microwave Stations to Relay Television Signals to Cmty. Antenna Sys., *First Report and Order*, Dkt. No. 14895, 38 F.C.C. 683, 699–700 (1965)).

Conversely, in *Echostar Satellite, LLC v. FCC*,[117] the D.C. Circuit held that the FCC could not exercise ancillary authority over satellite television encoding, as the Commission could not show that satellite television encoding was preventing the Commission from fulfilling its statutory responsibilities.[118] At issue was a congressional mandate to promote the commercial availability of cable set-top boxes.[119] The *Echostar* court rejected the FCC's assertion that the requirements for satellite providers promoted the statutory mandate to make cable set-top boxes commercially available.[120] Unlike *Southwestern Cable*, wherein the FCC found that CATV directly threatened its statutory mandate over broadcast television, the FCC showed no such connection in *Echostar*. The court noted that the only link between the satellite providers and the statute was a memorandum of understanding between the FCC and cable providers setting out the cable industry's commitment to future adoption of standards to promote competitive set-top boxes, and conditioned on the FCC requiring satellite MVPDs to adopt the same standard.[121]

Further adding to the body of ancillary authority jurisprudence, the D.C. Circuit clarified in *Comcast v. FCC*[122] that the FCC cannot rely on congressional statements of policy alone to support exercises of ancillary authority.[123] The FCC must instead rely on express congressional delegations of authority in the text of Titles II, III, and VI of the Act.[124] This confines the FCC's power to explicit statutory authorities, as opposed to broad assertions of policy that would potentially give the FCC unrestrained power in furtherance of those policy goals.[125] While this restraint on ancillary authority makes sense, on its face it prevents the FCC from regulating in ways that further the goals of Congress when changes in technology move faster than legislation.

---

117. Echostar Satellite, LLC v. FCC, 704 F.3d 992, 999 (D.C. Cir. 2013).

118. *Id.* at 998–1000.

119. *Id.* at 997–98; *see* 47 U.S.C. § 549(a) (Cable set-top boxes are termed "navigation devices.").

120. *Echostar Satellite*, 704 F.3d at 997–98.

121. *Id.* This memorandum of understanding was not agreed to by satellite MVPDs but imposed conditions on them through FCC rules.

122 . Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010).

123. *See id.* at 653–54; Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC (*NARUC I*), 533 F.2d 601, 612 (D.C. Cir. 1976). For an exhaustive discussion of pre-*Comcast* ancillary authority jurisprudence, *see* Werbach, *supra* note 102, at 571-77.

124. *Comcast*, 600 F.3d at 654 (internal quotation marks omitted).

125. *Id.* at 655–56.

E. The FCC's Authority in the Context of Rapid Technological Change

The FCC's ancillary authority is set against the backdrop of technological change.[126] Increasingly, our communications are conducted through the Internet, with the eventual goal of having an all-IP communications system.[127] One of the consequences of this transition to a new communications architecture is that it incentivizes telecommunications companies to shut down the old copper telephone network to avoid duplicative costs.[128] If a current telephone service provider shuts down its copper PSTN network and transfers all of the telephone traffic over IP links, the FCC could lose its authority to regulate the network via its Title II jurisdiction.[129] As the communications network transitions to Internet Protocol, the network consequently becomes more vulnerable to cyber-attacks and potentially more isolated from FCC authority.[130]

Because of the intertwining of an all-IP network and cybersecurity, securing Internet infrastructure poses questions about the scope of the FCC's authority over it. Recent D.C. Circuit decisions and FCC orders make it clear that if the FCC has authority to require that cybersecurity best practices be followed, that regulation must be grounded in some positive grant of statutory authority.

---

126. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 174–76 (1968) (approving of ancillary authority over a potentially disruptive new technology).

127. *See* Part II.A *supra* notes 42 and 43 and accompanying text (discussing the transition away from the copper PSTN to platform agnostic internetworking to transport voice, video, and data communications); *see also* PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, NETWORK SECURITY VULNERABILITY ASSESSMENTS TASK FORCE REPORT (Mar. 2002) [hereinafter NSVASTF REPORT], *available at* https://www.hsdl.org/?view&did=1540; Werbach, *supra* note 102, at 588.

128. Sean Buckley, *PSTN-to-IP Migration Must Be Done with Care, Say Verizon, AT&T*, FIERCETELECOM (May 15, 2012), http://www.fiercetelecom.com/story/pstn-ip-migration-must-be-done-care-say-verizon-att/2012-05-15; *see also* AT&T Petition to Launch Proceeding Concerning The TDM-to-IP Transition, WC Docket No. 12-353 (2012).

129. *See* Part II, *supra* notes 22-24; *see generally* Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 FED. COMM. L.J. 203, 234–61 (2014) (noting that many regulatory requirements for the PSTN do not hold after the IP transition, and making recommendations for which aspects of the PSTN should carry over to the new IP network, including universal service and reliability in this recommendation).

130. NSVASTF REPORT, *supra* note 127; Werbach, *supra* note 102, at 588. This becomes more clear as people increasingly use Internet services as their primary method of communication. *See* Outage Reporting to Interconnected Voice over Internet Protocol Serv. Providers, *Report and Order*, FCC 12-22, para. 2 (2012) [hereinafter VoIP Outage Order] (noting that about 27 million people had VoIP residential telephone subscriptions as of December 31, 2010); Cablevision Sys. Corp. v. FCC, 597 F.3d 1306, 1323 (D.C. Cir. 2010); Buckley, *supra* note 128.

III. THE FCC'S ANCILLARY AUTHORITY TO PROMULGATE CYBERSECURITY STANDARDS

There has been little discussion of the FCC's authority to create cybersecurity standards. In the realm of cybersecurity, authors have acknowledged that today's hodgepodge method of trying to ensure network infrastructure security is not working.[131] Members of Congress have introduced numerous bills to promote cybersecurity.[132] As evidenced by the introduction of these bills and the history of cybersecurity regulatory attempts, it is currently unclear which agency should be taking the lead. Furthermore, fear of regulation has foreclosed discussions of private industry regulation.[133] This Note shows a possible solution to this problem of insufficient cybersecurity by detailing a basis of FCC authority to require ISP implementation of cybersecurity best practices that result in increased reliability.

Evidence that poor cybersecurity impedes the actualization of statutory obligations would support the FCC's authority to create cybersecurity standards for ISPs. Because of the impact that cyber-attacks can have on the national communication infrastructure, the FCC could take regulatory action to prevent the disruption of those networks. As a federal agency, the FCC would first have to consider avenues of direct authority; however, the Communications Act does not directly authorize the FCC to implement cybersecurity regulations.[134] The Commission would therefore have to rely on its ancillary authority to implement any such regulations.

The ability of the FCC to exercise its ancillary authority depends on whether: (1) the service to be regulated falls within the FCC's Title I grant;

---

131. Karson K. Thompson, Note, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEX. L. REV. 465, 491 (2011) (stating that cybersecurity policy must be uniform and come from the top down because this structure eliminates the problems inherent in asking individual agencies to develop their own security strategies, such as a lack of uniformity and consistency). Other commenters assert that problems with cybersecurity manifest primarily in stolen data and not in problems with communications reliability. *See* Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEX. L. REV. 87, 87 (2012). While many cyber-attacks result in a loss of data, the same methods that are used to compromise the network to steal the information can be used to disrupt the network. *Id.*

132. *See, e.g.*, Cybersecurity Enhancement Act of 2013, H.R. 756, 113th Cong. (2013); Cybersecurity and Internet Safety Standards Act, S. 372, 112th Cong. (2011); Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. (2011); *see also* Thompson, *supra* note 131, at 482-88 (discussing seven cybersecurity proposals in the 112th Congress).

133. *See* Shane, *supra* note 131, at 91.

134. *See generally* 47 U.S.C. §§ 151-1473; *see also supra* text accompanying notes 90-93 (discussing FCC authority over broadband Internet).

and (2) the regulations are reasonably ancillary to the effective performance of a statutory mandate.[135]

A. Broadband Internet Service as Within the FCC's General Jurisdictional Grant

The FCC's general jurisdictional grant under Title I likely covers cyber-attacks and corresponding regulation of broadband Internet if these attacks are transmitted over an interstate all-IP communications network.[136] Title I gives the Commission jurisdiction over "interstate . . . communication by wire or radio."[137] Cybersecurity, or the lack thereof, affects both interstate communications by radio or wire and the Internet as a national network. The Supreme Court in *Southwestern Cable* set a low threshold for a service to fall within the Commission's Title I authority.[138] There, the Court found that cable systems carry programming made for a national audience, and so constituted interstate communications.[139] Today, Internet traffic has a worldwide reach; even if it is within an autonomous network, Internet traffic likely travels across state lines.[140] Furthermore, the general content of the traffic could be intended for a national audience. Cyber-attacks, in particular, have interstate and international character.[141] In a recent cyber-threat analysis, Mandiant, an information technology security company, found 115 instances of attacks originating from China from 2006 to 2012. [142] Because of the interstate and international characteristics of Internet traffic and disruptions, cybersecurity regulations fall within the FCC's Title I jurisdiction.

B. Mandatory Cybersecurity Standards for ISPs as Reasonably Ancillary to the FCC's Statutory Responsibilities

The creation of cybersecurity standards is reasonably related to the FCC's effective performance of its statutorily mandated responsibilities.[143] In the past, courts have upheld FCC assertions of ancillary authority when the regulated technology affected communications networks such as

---

135. Am. Library Ass'n v. FCC, 406 F.3d 689, 691–92 (D.C. Cir. 2005).

136. *See* 47 U.S.C. § 152 (2006); *see also* VoIP Outage Order, *supra* note 130, at paras. 60-61.

137. 47 U.S.C. § 152 (2006).

138. United States v. Southwestern Cable Co., 392 U.S. 157, 175–76 (1968).

139. *Id.*

140. *See* CSRIC III WORKING GROUP 6, SECURE BGP DEPLOYMENT 12 (Mar. 2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Final-Report.pdf.

141. *See, e.g.*, MANDIANT REPORT, *supra* note 15, at 22.

142. *Id.* These intercontinental attacks necessitate the utilization of interstate communication. *See id.* at 21.

143. *See* Am. Library. Assoc. v. FCC, 406 F.3d 689, 691–92 (D.C. Cir. 2005).

broadcast television and the telephone network.[144] For example, in *Southwestern Cable*, the order at issue was designed to remedy aspects of CATV, a new technology that had the potential to frustrate FCC obligations to ensure the continued viability of the broadcast television medium.[145]

Title 47 of the United States Code obligates the FCC to perform myriad other functions, including the creation of regulations for common carriers, rules for interconnection between telecommunications carriers, rules to ensure 9-1-1 services, and regulations to promote diversity of information sources and services provided in cable communications.[146] Furthermore, the FCC has a general obligation to make available "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense [and] promoting safety of life and property."[147] These are some of the core functions of the FCC. But a transition from a Title II to a Title I classification of the nation's communications system jeopardizes core FCC regulatory powers that exist only in Title II. If the FCC cannot exercise its Title II authority over the U.S. communications network, it must turn to ancillary authority, relying on the fact that an all-IP network without adequate cybersecurity safeguards could have disastrous effects on critical telecommunications and emergency services.[148]

These attacks have the potential to impair vital communications that the FCC oversees, such as telephony, Multichannel Video Programming Distributor ("MVPD") services,[149] and 9-1-1 functionality. FCC regulations requiring uniform implementation of cybersecurity best practices and updated network standards, such as those proposed by IETF and CSRIC, could mitigate the negative effects of these attacks on communications.[150]

Regulations aimed at ensuring the continuity of a communications service were examined in one of the seminal ancillary authority cases.[151] In *Southwestern Cable*, the Supreme Court upheld the FCC's exercise of ancillary authority because of CATV's potential to disrupt the broadcast television market.[152] Similarly, because of the possibility of communications disruption through the Internet, FCC mandatory cybersecurity standards are also reasonably ancillary to the FCC's effective

144. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 174–76 (1968); CCIA v. FCC, 693 F.2d 192, 210 (D.C. Cir. 1982).

145. *See Southwestern Cable*, 392 U.S. at 175.

146. *See* Part II.D, *supra* notes 75-79.

147. 47 U.S.C. § 151 (2006).

148. NSVASTF REPORT, *supra* note 127, at 65–66; *see, e.g.*, *See Zombies? Emergency Broadcast System Hacked*, *supra* note 50; Lee, *supra* note 51.

149. An MVPD is a cable, satellite, or IP-based service provider that distributes video programming. *See* 47 U.S.C. § 522(13).

150. *See supra* Part II.B.

151. *See* United States v. Southwestern Cable Co., 392 U.S. 157, 174–76 (1968).

152. *See id.*

performance of its statutorily mandated responsibilities of overseeing telephony, MVPD service, and 9-1-1 service. Furthermore, these attacks affect the FCC's general obligation to make available "a rapid, efficient, Nation-wide . . . wire and radio communication service," [153] where Congress has further required the FCC to make certain services available to the public, such as 9-1-1 service and broadband Internet. This is not to say that the FCC can regulate any communications platform at risk of a cyber-attack. The FCC would only be able to regulate the security of ISPs insofar as that insecurity poses a threat to the viability of functions the FCC is required to maintain.

Beyond interconnection and general network reliability, the FCC has a duty to promulgate regulations that ensure that Voice over Internet Protocol ("VoIP") providers give their users access to 9-1-1 service on parity with PSTN providers.[154] In doing so, the FCC can "take into account any technical, network security, or information privacy requirements that are specific to IP-enabled voice services."[155] Because cyber-attacks could disrupt 9-1-1 service on VoIP connections, requiring cybersecurity improvements is reasonably ancillary to the FCC's performance of its statutory obligations.

This situation does not suffer from the lack of a connection between the regulation and the service to be regulated seen in *Echostar*, where the FCC artificially conflated satellite service regulations with cable industry dealings.[156] The cyber-threats to the telecommunications networks are real; they were not created through jurisdictional bootstrapping.[157] Here, the FCC has ample evidence to support a finding that cyber-attacks could create a real obstacle to enforcement of its statutory obligation to ensure an efficient and reliable telecommunications network.

Since the FCC's inception, it has been obligated to ensure the efficiency of the nation's communications network.[158] Courts have consistently acknowledged that, as new technologies appear, the FCC must adapt.[159] And never before has the ability to disrupt our communications

153. 47 U.S.C. § 151 (2006).

154. 47 U.S.C. § 615a-1 (2006).

155. *Id.* This phrase represents an acknowledgement by Congress of the special security considerations that are necessary when transitioning to an all-IP communications infrastructure.

156. *See* Echostar Satellite, LLC v. FCC, 704 F.3d 992, 997-99 (D.C. Cir. 2013).

157. *See* Part II.D *infra*.

158. *See* 47 U.S.C. § 151 (2006).

159. *See, e.g.*, United States v. Southwestern Cable, 392 U.S. 157, 175–77 (1968) (noting that "Congress could not in 1934 have foreseen the development of community antenna television systems, but it seems to us that it was precisely because Congress wished 'to maintain, through appropriate administrative control, a grip on the dynamic aspects of radio transmission,' that it conferred upon the Commission a 'unified jurisdiction' and 'broad authority.' Thus, '(u)nderlying the whole (Communications Act) is recognition of the rapidly fluctuating factors characteristic of the evolution of broadcasting and of the

networks been so widely available.[160] Therefore, mandating standards is likely ancillary to the FCC's statutory responsibilities, and the FCC may use its ancillary authority to promulgate rules accordingly.

IV. THE DECISION TO REGULATE CYBERSECURITY OF INTERNET SERVICE PROVIDERS

Having concluded that the FCC likely has authority to regulate the cybersecurity practices of ISPs under its Title I ancillary authority, the question remains whether the FCC should exercise this authority. The FCC is the unifying authority for telecommunications regulation,[161] a status that reflects the belief that an administrative agency can adapt its regulations to changes in technology more quickly than Congress.[162] The FCC's relative nimbleness suggests that the FCC should play a role in cybersecurity. This has already been recognized to an extent in the the Presidential Policy Directive accompanying the Cybersecurity Executive Order, where the FCC is charged with coordinating with the communications sector in developing and implementing the Cybersecurity Framework.[163] It has superior institutional competence regarding communications networks in addition to its longstanding relationship with companies in the telecommunications industry. As more people and communications technologies use the Internet as their sole communications network, the FCC's obligations to ensure a reliable communications network will increasingly intrude on the Internet domain.

The FCC already has a good model for what cybersecurity standards should look like. CSRIC recommendations and finalized IETF security standards provide a trusted way of determining the standard with expertise.[164] Furthermore, the Cybersecurity Executive Order tasks NIST and DHS, with input from the FCC, with creating a Cybersecurity

---

corresponding requirement that the administrative process possess sufficient flexibility to adjust itself to these factors." (citations omitted)).

160. *See* NSVASTF REPORT, *supra* note 148, at 4, and accompanying text.

161. *Southwestern Cable*, 392 U.S. at 168.

162. *Id.* at 172-73.

163. Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, Feb. 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (directing the FCC to "exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends").

164. *See* CSRIC Press Release, *supra* note 61, at *2; Bush, *supra* note 38.

Framework for the private sector to implement.[165] The implementation of the Framework could improve cybersecurity as well. With these resources in mind, this section of the Note addresses whether the FCC should regulate the cybersecurity of ISPs.

Deciding whether and how to regulate can be a hard choice for agencies to make, especially given the wide discretion they are afforded. The calculus involves two separate inquiries. Initially, the agency must decide whether to regulate, which involves an evaluation of agency goals and the problem the agency seeks to address, along with a determination of whether the problem lends itself to a regulatory fix.[166] After determining that regulatory action is appropriate, the agency must analyze the costs and benefits of different regulatory alternatives and choose the best one.[167]

This Part's analysis first focuses on resolving the dilemma of whether the FCC should regulate ISPs' cybersecurity practices in the first place. The contrasting options are relatively straightforward: impose regulation that will result in basic infrastructure cybersecurity protections or choose not to regulate and instead let the market provide the level of protection its participants deem necessary. This Part then briefly considers the basic cost-benefit analysis and offers recommendations on how to apply that analysis to the problem of protecting network infrastructure from cyber-attacks.

A. Deciding When to Regulate

1. Appropriate Considerations for Deciding When to Regulate

In 2003, the Office of Management and Budget issued a circular to help guide agency decisions of whether and how to regulate.[168] It recognized that good regulatory analysis requires justifications of the need for the proposed action.[169] This Part's description of the initial determination of whether to regulate borrows heavily from the circular.

---

165. Cybersecurity Executive Order, *supra* note 64, at 11,739-41.

166. *See* OFFICE OF MGMT. & BUDGET, CIRCULAR A-4: A REGULATORY ANALYSIS, at 3–5 (2003) [hereinafter Circular A-4], *available at* www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a004/a-4.pdf.

167. *See id.* at 2.

168. *See generally id.* These principles have been reaffirmed by the Obama Administration in recent Executive Orders. *See* Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 21, 2011) (President Obama) (stating that the benefits of proposed and final rules must "justify" the costs); Exec. Order No. 13,579, 76 Fed. Reg. 41,587 (Jul. 14, 2011) (stating that independent regulatory agencies "should promote" the goals expressed in EO 13,563); *see also* BENEFIT-COST ANALYSIS AT INDEPENDENT REGULATORY AGENCIES COMMITTEE ON REGULATION, ADMINISTRATIVE CONFERENCE OF THE UNITED STATES (Apr. 23, 2013) (draft recommendation), *available at* http://www.acus.gov/sites/default/files/documents/IRC%20BCA%20Recommendation%20for%204-29-13%20Mtg%20FINAL.pdf.

169. *See id.* at 2.

The determination of the need for the regulatory action incorporates the statutory or judicially recognized basis for the action and considers the specific conditions that generate the need for action.[170] When not explicitly mandated by law, regulatory action is warranted when there is a compelling need for action.[171] Examples of compelling needs include remedying material failures of private markets to protect or improve public health, safety, and well-being, and meeting other compelling public needs such as "promoting intangible values such as distributional fairness or privacy."[172] Finally, this assessment involves a tentative determination of the effectiveness of government action, including whether any proposed government regulation would do more good than harm.[173] To satisfy this last factor, the agency must overcome a presumption against economic regulation.[174] The legal authority for any potential cybersecurity regulation was discussed in the preceding sections.[175] Accordingly, this section will focus on the other aspects of agency decision-making.

a. *Market Failures and Other Compelling Needs*

Market failures occur for three primary reasons: externalities, abuse of market power, and inadequate or asymmetric information.[176] Externalities allow one party to "impose uncompensated benefits or costs on another party."[177] A firm with a dominant position in a market abuses its market power when it increases the price or reduces the output of its products so as to earn profits in excess of what would be attainable in a competitive market.[178] Inadequate information creates a market failure when it inhibits producer or consumers from making informed decisions about their participation in the market.[179] This allows actors with superior information to use it to their benefit or to the detriment of those without

170. *See id.* at 3–4 (citing Executive Order 12866, which states that "Federal agencies should promulgate only such regulations as are required by law, are necessary to interpret the law, or are made necessary by compelling need, such as material failures of private markets to protect or improve the health and safety of the public, the environment, or the well being of the American people"). The previous sections of this Note discuss the legal basis for regulatory action relying on the Commission's ancillary authority. *See* Part III *supra*.

171. Executive Order 12866 §1(a).

172. *See* Circular A-4, at 4.

173. *Id.*

174. *Id.* at 6.

175. *See* Part III *supra*.

176. *See* Circular A-4, at 4.

177. *See id.*

178. *See id.* at 4–5.

179. *See generally* Aidan R. Vining & David L. Weimer, *Information Asymmetry Favoring Sellers: A Policy Framework*, 21 POLICY SCIENCES 281 (1988).

information.[180] For example, a food producer is in a much better position to know the quality and ingredients of its food than the would-be buyer. The producer could use this information to induce the consumer to pay a higher price for food than she would otherwise if she had known the true quality and ingredients of the food.[181] However, when the information available to participants in a market is incomplete, market failure does not necessarily result. The primary generator or holder of relevant information need not always serve as the supplier of that information; it may also be provided by third parties.[182] This does not, however, mean that when information is available, it will be adequate to remedy a market failure, because of the inability of the public or other market participants to process the information in a relevant way. This most often "occurs in cases of low probability, high-consequence events."[183] Furthermore, "[w]hen it is time-consuming or costly for consumers to evaluate complex information about products or services . . . , they may expect government to ensure that minimum quality standards are met."[184]

Circular A-4 recognizes that situations other than market failures can provide compelling justifications for regulations.[185] Examples include congressionally created programs to redistribute resources or ensure efficient, non-discriminatory distribution of resources.[186] Other examples include regulation to protect privacy, permit more personal freedom, or promote other democratic considerations.[187]

b. *Federal Regulation as the Best Method to Solve the Problem*

Even when the above concerns exist and create the problem, an agency should consider alternatives to regulation, including antitrust enforcement, consumer-initiated product liability lawsuits, administrative compensation systems, and state regulation or enforcement.[188] When considering regulation, agencies must be cognizant of the presumption against economic regulation.[189] A high burden of proof must be met to demonstrate the need for "mandatory uniform quality standards for goods or services if the potential problem can be adequately dealt with through

180. *See id.* at 291–98 (detailing situations where information asymmetries create market failures and giving suggestions for government interventions in appropriate circumstances).
181. Circular A-4, *supra* note 166,at 5.
182. *Id.*
183. *Id.*
184. *Id.*
185. *See id.*
186. *See id.*
187. *Id.*
188. *Id.* at 6.
189. *Id.* at 7.

voluntary standards or by disclosing information of the hazard to buyers or users."[190]

2. The Decision to Regulate Cybersecurity to Ensure Network Reliability

Both a market failure and a compelling need for a reliable communications network justify regulating insufficient ISP cybersecurity and network reliability. While such regulation can engender concerns of government overreach through economic regulation, well-thought-out federal regulation is the best way to solve the problem. The Commission should regulate broadband Internet Service Providers' cybersecurity measures to increase network reliability. This subsection addresses each justification in turn.

a. *Market Failure Through Inadequate Information*

Network reliability and cybersecurity are susceptible to problems resulting from inadequate information, both for consumers and governments. Part II of this Note documented the failings of only some of the standard protocols through which the Internet operates; the reality of computer vulnerabilities is that they are numerous and hard to discern.[191] Further, most network operators do not make their downtime statistics available to the public or the FCC.[192] It is therefore hard to measure how often the network is unavailable to consumers. If consumers and the government had data on vulnerabilities and network downtime, they could demand a more reliable network that is hardened against future attacks. This lack of information creates a market failure, inasmuch as consumers

190. *Id.*

191. See Dan Assaf, Government Intervention in Information Infrastructure Protection, in IFIP International Federation for Information Processing, Vol. 253, (E. Goetz & S. Shenoi eds.) 35–38 (2008) (noting a lack of cybersecurity information sharing between actors in the private sector). Further, many cyber-attacks rely on "zero-day vulnerabilities," which are previously unknown computer flaws. *See* McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 686 (2012); Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?* 35 FORDHAM INT'L L.J. 842, 853-54 (2012).

192. Many telecommunications companies strongly disapprove of releasing network outage reporting data already collected by the FCC through the NORS and 9-1-1 reliability program to the public. *See, e.g.*, Improving 911 Reliability, *Report and Order*, FCC 13-158, 28 FCC Rcd. 17476, para. 153. (2013) [hereinafter *911 Reliability Order*]. While not the focus of this Note, many web services do publish service availability information, including historical data. See, for example, http://status.aws.amazon.com/ and http://www.google.com/appsstatus#hl=en&v=status&ts=1395719999000.

cannot accurately assess the risks of network vulnerabilities and cannot appraise the value of the service accordingly.

Further, it is unclear if a traditional market model applies in the case of the Internet, given the differences between last mile connections and general network infrastructure. While network infrastructure is shared and used by everyone who traverses the network, the market for last mile connectivity is in many places a monopoly for consumers.[193] Further, because of common utilization, the origins and destinations of the traffic on this segment of the network are most likely connected by numerous different paths.[194] This characteristic makes the network infrastructure as a whole less vulnerable to failure, assuming no vulnerability is shared by the operators of multiple paths. However, given that a single manufacturer dominates the market for network switches and that the aforementioned vulnerabilities afflict many protocols that virtually all network operators use, it is likely that vulnerabilities do exist.[195]

Network packets can take multiple different paths, so ISPs do not have incentives to upgrade the security on their networks or make them more reliable because increased information is less likely to impact consumers' choices in ISPs. However, individual ISPs do have limited control over the network infrastructure and over which path data takes to get to its destination. While ISPs can and do route their traffic to different networks with differing priorities,[196] it is unclear if they have the knowledge or the incentive to route traffic to more secure networks. Because of the lack of information accessible to the public about cyber vulnerabilities, the FCC should conclude that a market failure justifies a decision to regulate. There is, however, a stronger rationale that justifies regulation of ISPs' cybersecurity practices—the compelling need for a reliable communications network.

---

193. *See generally* SUSAN CRAWFORD, CAPTIVE AUDIENCE: THE TELECOM INDUSTRY AND MONOPOLY POWER IN THE NEW GILDED AGE (2013) (arguing that residentially broadband users have essentially one choice for high speed Internet).

194. *See* Inquiry Concerning the Deployment of Advanced Telecomms. Capability to All Americans in A Reasonable & Timely Fashion, *Second Report*, FCC 00-290, CC Docket No. 98-146, 15 FCC RCD. 20913, 20922-23, paras. 17-18 (2000).

195. *See* Part II *supra* (discussing BGP and DNS); Ahsan Aslam Khan, *Cisco's Clear Dominance in Data Networking*, THE MOTLEY FOOL (June 25, 2013) http://www.seattlepi.com/business/fool/article/Cisco-s-Clear-Dominance-in-Data-Networking-4486272.php (noting that Cisco Systems has over 60% of the market share for routers and switches); Snowden, *supra* note 4.

196. That is, Comcast might have a more favorable traffic payment arrangement or peering with certain backbones, and would preferentially divert traffic to those networks if possible, at the expense of using other potential paths to get its traffic to the same destination. *See generally* Daniel Golding, *The Real Story Behind the Comcast-Level 3 Battle*, GIGAOM (Dec. 1, 2010), http://gigaom.com/2010/12/01/comcast-level-3-battle/.

b. *Compelling Need for a Reliable Nationwide Communications Network*

As early as 1934, with the passage of the Communications Act, Congress recognized the importance of a reliable, nationwide communications network.[197] The purpose of the FCC is to ensure "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities . . . for the purpose of the national defense [and] promoting safety of life and property."[198] The FCC has realized its purpose with the telephone network, and to a lesser extent with the Internet. Both have immensely increased the productivity and prosperity of the United States.[199]

Although the word "reliable" is not in section 151, it is implied by our dependence on the interstate and international communications network. Much of our daily communications traverse the Internet, from phone conversations converted to VoIP and back to the PSTN to entertainment and banking. The Internet has provided significant benefits to society and countless new ways to communicate.[200] With regard to public disasters, the FCC has recently shown a desire to improve network reliability, indicating that this is an essential aspect of the communications network.[201] The promotion of a reliable communications network serves intangible values such as public safety and national security. The FCC recently expounded upon this idea in an order requiring increased reliability and certification oversight for service providers to 9-1-1 public-safety answering points.[202] This compelling need would likely justify government regulation of the cybersecurity practices of ISPs even if there were not a market failure caused by a lack of information.

c. *Federal Regulation as the Best Way to Ensure a Reliable Communications Network*

Even if remedying vulnerabilities in the communications network is justified by a market failure or a compelling need, the FCC must consider

---

197. 47 U.S.C. § 151 (2006).

198. 47 U.S.C. § 151 (2006).

199. *See* REED HUNDT & BLAIR LEVIN, THE POLITICS OF ABUNDANCE ch. 2 (2012).

200. *See* HUNDT & LEVIN, *supra* note 199, ch. 2 (noting the benefits of the Internet and making recommendations to improve society through future technologies that take advantage of this interconnectedness).

201. *See generally* Improving the Resiliency of Mobile Wireless Commc'ns Networks, *Notice of Proposed Rulemaking*, Release No. FCC 13-125, (2013), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-13-125A1.pdf (introducing measures to increase transparency to consumers regarding the ability of different wireless service providers to maintain their networks operational during emergencies); *911 Reliability Order*, *supra* note 192 (adopting rules to ensure that 911 communications networks nationwide are dependable and resilient).

202. *See 911 Reliability Order*, *supra* note 192, paras. 1-6.

other options before making a decision to regulate. Many of the alternative options suggested by the Office of Management and Budget in the A-4 Circular cannot remedy the problem of network reliability. This is not an antitrust issue, nor is it a products liability issue.[203] The Internet and nationwide communications network are archetypical interstate systems and are not amenable to regulation by the states.[204] These considerations all weigh heavily in favor of federal regulation.

However, the FCC should be mindful of the presumption against economic regulation.[205] It is possible that FCC regulation would take the form of mandatory, uniform quality standards for goods or services. This type of regulation requires a hard look at its necessity. Specifically, the FCC must consider whether "the potential problem can be adequately dealt with through voluntary standards or by disclosing information of the hazard to buyers or users."[206] This is the most significant criticism of FCC regulation.

If ISPs start to disclose their security practices, consumers may choose the best security among service providers, providing an incentive for ISPs to compete for customers over the issue of cybersecurity. While recent disclosures of network vulnerabilities provide some information about the state of cybersecurity to consumers,[207] there is no indication that ISPs are planning to compete in this arena. The FCC's Cyber Security Certification Program Notice of Inquiry might have also provided information to consumers, however, that docket has not been revisited since 2011.[208] Voluntary cybersecurity and network reliability commitments may be an adequate solution to this problem, and the FCC has moved in this direction. The Communications Security, Reliability and Interoperability Council already convened by the FCC is one avenue to encourage network operators to make voluntary commitments. Indeed, the FCC has secured voluntary commitments from many of the largest Internet service providers to address vulnerabilities with DNS and BGP,[209] and

---

203. See RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19 (1998) (stating that services, "even when provided commercially, are not products," and so are not subject to the rules of products liability).

204. Indeed, the Communications Act "must be construed in light of the needs for comprehensive regulation and the practical difficulties inhering in state by state regulation of parts of an organic whole." Gen. Tel. Co. of Cal. v. FCC, 413 F.2d 390, 398 (D.C. Cir. 1969). The whole point of the Federal Communications Commission is to regulate the communications industry. ON/TV of Chicago v. Julien, 763 F.2d 839, 842 (7th Cir. 1985).

205. Circular A-4, *supra* note 166, at 6.

206. *Id.* at 7.

207. The NSA disclosures provide a wealth of data on the state-of-the-art intrusion techniques used by the U.S. Government. Some of these techniques targeted ISPs with previously unknown cybersecurity vulnerabilities.

208. Cyber Sec. Certification Program NOI, *supra* note 53.

209. *See* FCC Advisory Committee Adopts Recommendations to Minimize Three Major Cyber Threats, *supra* note 61, at 1. However, as noted in Part II.C, these commitments cover only fifty percent of residential broadband users. *Id.*

CSRIC IV will be making recommendations for voluntary adoption of other cybersecurity best practices in conjunction with the NIST Cybersecurity Framework.[210]

However, not all cybersecurity problems that threaten network reliability can be solved in such a manner; a recent proceeding addressing 9-1-1 reliability shows why. Over the last ten years, the Commission had relied on assurances by 9-1-1 service providers that they would voluntarily implement industry best practices such as backup power and connection diversity for public-safety answering points.[211] When considering the causes of 9-1-1 service failures, the FCC determined that the adoption of these industry best practices could have prevented the 9-1-1 outages experienced during and after the 2012 derecho; unfortunately, that implementation did not happen.[212] This is a clear example that reliance on voluntary commitments to adopt these best practices did not produce the reliability needed for this service.[213] With cybersecurity, voluntary commitments by ISPs may also result in lack of implementation, especially given the lackadaisical adoption of DNSSEC noted above.[214] The FCC must also consider the feasibility of obtaining commitments from all service providers. Furthermore, will these commitments encompass new vulnerabilities and changing technology? Will these commitments actually ensure reliability? These are difficult questions, and the gravity of ensuring the safety of our economy militates toward obtaining more certain assurances that reliability is paramount.

Ensuring high reliability and protection from cyber-attacks on the communications infrastructure may be possible only with regulation. Having concluded that the FCC should regulate, this Note now turns to a brief discussion of the FCC's considerations for *how* it should regulate.

B. Cost-Benefit Analysis and Cost-Effectiveness Analysis

Once an agency has decided to regulate, it must choose the best method of regulation to achieve its goal. Cost-benefit analysis and cost-effectiveness analysis are prominent methodologies to help agencies make this choice.[215] As the influential scholar and Supreme Court Associate Justice Stephen Breyer wrote, cost-benefit analysis embodies "a simple axiom for creating and implementing any program: determine the

---

210. CSRIC IV, *supra* note 69, at 5.

211. *See 911 Reliability Order*, *supra* note 192, paras. 11-14.

212. *See id.* at para. 21.

213. *Id.* at paras. 24-26 (noting that "service providers may choose–and have chosen–to disregard these voluntary recommendations, even when they concern critical 911 services").

214. *See* Part II.A *supra*.

215. Circular A-4, *supra* note 166, at 9; *see generally* Cass R. Sunstein, *Cost-Benefit Default Principles*, 99 MICH. L. REV. 1651, 1662 (2001). The initial description here applies to both cost-benefit analysis and cost-effectiveness analysis, even if cost-benefit analysis is the methodology mentioned by name.

objectives, examine the alternative methods of obtaining these objectives, and choose the best method for doing so."[216] Cost-benefit analysis is a way of producing a full appraisal of a proposal that reflects the shortcomings inherent in the human decision-making process.[217] In addition, cost-benefit analysis forces agencies to explicitly state their rationale for regulating. By articulating the basis for the decision, agencies allow the public an opportunity to provide input in a way not necessarily required by the minimum notice and comment procedures.[218]

In 1993, President Bill Clinton issued an Executive Order setting out general principles of regulation.[219] These have been lauded as a codification of the principles of cost-benefit analysis,[220] and subsequent guidance from the Office of Management and Budget has expanded upon the principles in the Executive Order.[221] While the FCC, as an independent agency, is not obligated to take these considerations into account or to obtain Office of Information and Regulatory Affairs ("OIRA") approval before it promulgates regulations,[222] these principles provide an excellent foundation to guide the decision of whether or not to mandate cybersecurity standards.[223] Summarizing the principles produces several overarching considerations:

---

216. STEPHEN G. BREYER, REGULATION AND ITS REFORM 5 (1982).

217. *See* Sunstein, *supra* note 215, at 1662 (observing that people "have difficulty in calculating probabilities, and they tend to rely on rules of thumb, or heuristics, that can lead them to make systematic errors . . . in thinking about the seriousness of certain risks.").

218. *Id.*; *see also* Michael A. Livermore & Richard L. Revesz, *Regulatory Review, Capture, and Agency Inaction*, 101 Geo. L.J. 1337, 1370 (noting that the cost-benefit analysis methodology reduces agency capture through "requiring the examination of a wide range of regulatory effects; . . . [being] standardized and supported by a set of professional norms; and . . . improv[ing] transparency, by publishing for public scrutiny agency estimates of regulatory effects.").

219. Exec. Order 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993).

220. *See* Sunstein, *supra* note 215, at 11655-656. More recently, Commissioner Maureen Ohlhausen drew upon the principles and adapted them to form principles for when the Federal Trade Commission should use its unfair methods of competition authority to regulate. *See Section 5: Principles of Navigation*, Remarks of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission at the U.S. Chamber of Commerce (Washington, D.C., July 25, 2013).

221. *See* Circular A-4, *supra* note 156, at 1.

222. *See* Exec. Order 12,866, 58 Fed. Reg. §6(a)(3). To reduce the paperwork burden businesses, people, and small governments, the FCC does have to submit proposed regulations to OMB when obtaining information from ten or more persons. *See* 5 C.F.R. §§ 1320.3, 1320.4.

223. Exec. Order 12,866, 58 Fed. Reg. §1(b). Not every principle applies in this analysis. For reference the twelve principles are:

> (1) Each agency shall identify the problem that it intends to address (including, where applicable, the failures of private markets or public institutions that warrant new agency action) as well as assess the significance of that problem.
> (2) Each agency shall examine whether existing regulations (or other law) have created, or contributed to, the problem that a new regulation is

1. Identify the problem that the regulation seeks to address.

---

intended to correct and whether those regulations (or other law) should be modified to achieve the intended goal of regulation more effectively.
(3) Each agency shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public.
(4) In setting regulatory priorities, each agency shall consider, to the extent reasonable, the degree and nature of the risks posed by various substances or activities within its jurisdiction.
(5) When an agency determines that a regulation is the best available method of achieving the regulatory objective, it shall design its regulations in the most cost-effective manner to achieve the regulatory objective. In doing so, each agency shall consider incentives for innovation, consistency, predictability, the costs of enforcement and compliance (to the government, regulated entities, and the public), flexibility, distributive impacts, and equity.
(6) Each agency shall assess both the costs and the benefits of the intended regulation and, recognizing that some costs and benefits are difficult to quantify, propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs.
(7) Each agency shall base its decisions on the best reasonably obtainable scientific, technical, economic, and other information concerning the need for, and consequences of, the intended regulation.
(8) Each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt.
(9) Wherever feasible, agencies shall seek views of appropriate State, local, and tribal officials before imposing regulatory requirements that might significantly or uniquely affect those governmental entities. Each agency shall assess the effects of Federal regulations on State, local, and tribal governments, including specifically the availability of resources to carry out those mandates, and seek to minimize those burdens that uniquely or significantly affect such governmental entities, consistent with achieving regulatory objectives. In addition, as appropriate, agencies shall seek to harmonize Federal regulatory actions with related State, local, and tribal regulatory and other governmental functions.
(10) Each agency shall avoid regulations that are inconsistent, incompatible, or duplicative with its other regulations or those of other Federal agencies.
(11) Each agency shall tailor its regulations to impose the least burden on society, including individuals, businesses of differing sizes, and other entities (including small communities and governmental entities), consistent with obtaining the regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations.
(12) Each agency shall draft its regulations to be simple and easy to understand, with the goal of minimizing the potential for uncertainty and litigation arising from such uncertainty.

2. Analyze the costs, benefits, and impacts on incentives for each alternative regulatory option, recognizing that some costs and benefits are difficult to quantify.
3. Choose the option in which the benefits best justify the costs, avoiding inconsistent or duplicative regulation.
4. Provide clear guidance for stakeholders and those affected by the proposed regulation.[224]

The FCC has shown implicit acceptance of these considerations when deciding whether to regulate.[225]

Cost-benefit analysis is not at odds with regulation, nor is it a purely economic approach to regulation.[226] Instead, it is an "instrument designed to ensure that the consequences of regulation are placed before relevant officials and the public as a whole, and intended to spur attention to neglected problems while at the same time ensuring that limited resources will be devoted to areas where they will do the most good."[227] It is important that agencies do not engage in cost-benefit analysis to the detriment of society by failing to come to a conclusion using cost-benefit tools.[228] This "paralysis by analysis" can prevent desirable regulations from going forward.[229]

1. Principles of Cost-Benefit Analysis and Cost-Effectiveness Analysis

The considerations of cost-benefit analysis and cost-effectiveness analysis fall along different axes. Cost-benefit analysis is used to compare regulatory options that have outcomes that can be measured in dollar values, while cost-effectiveness analysis looks to the efficacy of each potential regulatory measure.[230] If possible, agencies should perform both analyses when choosing among regulatory alternatives.[231] The background section of this Note identified the problem that the FCC must address. Having dispensed with the first step, the following discussion will focus on steps two through four.

---

224. *See id.*; Livermore, *supra* note 218, at 1370-71.
225. *See* Preserving the Open Internet, *Notice of Proposed Rulemaking*, FCC 09-93, 24 FCC Rcd. 13064, paras. 48-80 (2009) (discussing the need for Commission action by considering the goals of the Commission, the current state of broadband and the Internet marketplace, and the debate regarding traffic management pricing and practices).
226. *See* Sunstein, *supra* note 215, at 1663.
227. *Id.*
228. *Id*.
229. *Id.*
230. Circular A-4, *supra* note 166, at 10.
231. *Id.* at 9.

a. *Determining the Costs and Benefits of the Alternatives*

The agency must show how the proposed action will bring about the anticipated costs and benefits.[232] Cost-benefit analysis reduces both the costs and the benefits of proposed regulation to monetary units, thereby facilitating the evaluation of the proposal through a common metric.[233] Accordingly, the agency should show the monetized values of the benefits and costs to society.[234] When benefits are not amenable to measurement using monetary units, agencies must still try to measure the outcomes in terms of physical units.[235] When direct measurements of costs and benefits are not possible, either because the market does not exist or because the costs and benefits are intangible, an agency can use implicit price estimates,[236] revealed preference measures,[237] and stated preference measures[238] to determine a monetized value for goods and services. Costs and benefits are measured against a baseline of outcomes expected to occur if the regulation is not implemented.[239] This baseline must consider how the market will likely evolve and external factors affecting expected costs and benefits.[240] Agencies should generally analyze at least three options: "the preferred option; a more stringent option that achieves additional benefits (and presumably costs more) beyond those realized by the preferred option; and a less stringent option that costs less (and presumably generates fewer benefits) than the preferred option."[241]

Agencies must consider the costs of a regulation in addition to its benefits.[242] A regulatory approach that is blind to its costs reduces societal benefits in the aggregate, even if the regulatory goal has a higher positive effect in remediating the problem. Professor Cass Sunstein, former Administrator of the Office of Information and Regulatory Affairs, describes this principle in the context of environmental regulation:

---

232. *Id.* at 18.
233. *Id.* at 10.
234. *Id.* at 18.
235. *Id.* at 10.
236. *Id.* at 20.
237. *Id.* at 20–21. One caveat for the revealed preference measure is that it requires a well-informed market participant to obtain accurate measures. *Id.* This may pose difficulties when measuring reveal preference for cybersecurity and network reliability. *Id.*
238. *Id.* at 22–23.
239. *Id.* at 15–16.
240. *Id.* at 15.
241. *Id.* at 16.
242. While this may seem intuitive and will certainly be brought up by the regulated entities, it is important to see its rationale, as it focuses agency efforts. Sunstein, *supra* note 215 (explaining the rationale for considering both costs and benefits in addressing agency efforts).

> The basic idea is that a "benefits only" approach also reflects a kind of tunnel vision, a myopic focus on only one of the variety of things that matter. Suppose, for example, that one approach to regulation would produce a certain level of air quality benefits, but at a cost of $800 million, and that a competing approach would produce a trivially lower level of air quality benefits, but at a cost of $150 million. If costs can be made relevant, the agency is permitted to do what seems quite sensible: save the $650 million, because the benefits would not be high enough to justify the expenditure.[243]

This approach leads to more rational regulation.[244]

When determining costs and benefits, there are a number of considerations suggested by Executive Order 12866.[245] One common measure of cost is the economic criterion of the "private willingness to pay."[246] This is a measure of how much individuals would be willing to forgo to enjoy a particular benefit.[247] However, this measure suffers from a number of deficiencies. Willingness to pay depends on having information about the problem and its consequences and the means to pay once the consequences of maintaining the status quo are known.[248] Further, private willingness to pay does not necessarily take into account intangible costs and benefits that society as a whole would receive from a regulation.[249] Accordingly, this should be one factor among many considered, including the measures mentioned above such as implicit price estimates, revealed preference measures, and stated preference measures.

Another consideration is a "feasibility requirement," which considers whether it is feasible for the regulated industry to implement the regulation.[250] However, at its heart, a feasibility requirement involves no balancing of costs and benefits.[251] This is because any "significant increase in costs is likely to prove 'not feasible' for at least some companies."[252] Using the "feasibility requirement" is appropriate in extreme cases, i.e. a regulation is infeasible if it significantly harms the industry resulting in

---

243. *Id.* at 1691.

244. *See id.* at 1684 (noting that "Justice Breyer expressly endorses the default rule of *Michigan v. EPA*, saying that in the face of statutory ambiguity, agencies should be allowed to consider costs, if only because that approach would increase the likelihood of rational regulation.").

245. *See* Exec. Order 12,866, 58 Fed. Reg. 51,735 § 6(a)(3)(C) (Sept 30, 1993).

246. See Sunstein, *supra* note 215, at 1661.

247. Circular A-4, *supra* note 166, at 18.

248. Sunstein, *supra* note 215, at 1661.

249. *See id*.

250. *See id.* at 1701.

251. *Id.* (citing Am. Textile Mfrs. Inst. v. Donovan, 452 U.S. 490 (1981)).

252. *See* Sunstein, *supra* note 215, at 1701.

"large numbers of business failures, substantial losses of jobs, or the equivalent."[253]

When possible, agencies should use market data about the actual prices for the goods or services affected by regulation.[254] Market prices provide good data for estimating costs and benefits if the services affected by the regulation are traded in a "well-functioning competitive market."[255] For many costs, it may be difficult to quantify the consequences of either regulating or not regulating.[256] Regardless of whether they are quantifiable, though, these costs and benefits must be considered.[257] Qualitative measures for assessing the consequences of inaction or regulation include "distributive impacts" and "equity" analyses.[258]

When analyzing non-quantified costs and benefits, the agency must carefully describe these intangibles *qualitatively*.[259] The agency must "present any relevant quantitative information along with a description of the unquantifiable effects, such as . . . improvements in quality of life . . . [with] a discussion of the strengths and limitations of the qualitative information."[260] This description should also include reasons why the information cannot be quantified.[261]

b. *Cost-Effectiveness Analysis*

Cost-effectiveness analysis is used to identify the most effective uses of resources, comparing different regulatory actions with the same primary outcome.[262] The most cost-effective regulatory alternative is the one that achieves the best outcome at a reasonable or threshold cost; it is not necessarily the alternative with the highest cost-to-effectiveness ratio.[263] To perform the analysis, an agency must carefully construct the cost and performance measures (effectiveness) for the regulatory alternatives.[264] Cost is the net cost of the regulation, subtracting cost savings (though not primary outcomes) from the costs of the regulation.[265] Effectiveness

253. *Id.* at 1702–03 (citing United Steelworkers of Am. v. Marshall, 647 F.2d 1189 (D.C. Cir. 1980); Bldg. & Constr. Trades Dep't. v. OSHA, 838 F.2d 1258 (D.C. Cir. 1988); Nat'l Cottonseed Prods. Ass'n v. Brock, 825 F.2d 482 (D.C. Cir. 1987)).

254. *See* Circular A-4 *supra* note 166, at 21-22.

255. *Id.* at 19.

256. *See* Exec. Order 12,866, 58 Fed. Reg. 51,735 §1(b)(6) (Sept. 30, 1993).

257. *See id.*

258. *See id.* § 1(a), (b)(5).

259. *See* Circular A-4, *supra* note 166, at 27.

260. *Id.*

261. *Id.* (Here, OMB specifically identifies situations where the "existence of a risk may be based on highly speculative assumptions, and the magnitude of the risk may be unknown" as circumstances where quantization may be difficult and qualitative description may be needed).

262. *Id.* at 11

263. *Id.*

264. *Id.*

265. *Id.*

measures are the final outcomes of the regulation.[266] Effectiveness measures should examine how a regulation reduces the severity and the duration of the problem it seeks to remedy.[267]

FCC analysis will likely require the use of both cost-benefit analysis and cost-effectiveness analysis. Cybersecurity and network reliability seem particularly amenable to cost-effectiveness analysis because different regulatory measures would have the same outcome of increased network reliability.

2. Application to Cybersecurity Standards

It may be difficult to quantify and account for all of the costs and benefits associated with increased reliability and decreased vulnerability to cyber-attacks that threaten network infrastructure. The FCC will need to devote time and resources to considering the various factors involved and providing appropriate opportunities for public comment. This subsection provides some initial considerations for this analysis.

Direct costs of cybersecurity regulation will likely include upgrade costs for service providers, wages for more security and network analysts who can determine vulnerabilities, and funds spent to ensure administrative compliance with regulations. Insofar as providers spend money to comply with cybersecurity regulation, those funds might have otherwise enabled other infrastructure upgrades, such as increased bandwidth and connection speeds. These costs could be passed down to consumers, so the analysis should account for ancillary costs such as decreased access to the network by lower income groups.

Tangible benefits of increased cybersecurity and network reliability include improved economic activity through decreased downtime and improved national security. Intangible benefits include increased trust in the communications system. Qualitative descriptions can sometimes replace exact cost-benefit monetization, especially for intangible aspects and for events that are low-probability but high-consequence occurrences. Here, a network failure due to cybersecurity vulnerabilities is an example of a low-probability, high-consequence event. As such, the FCC should ensure it addresses all of the considerations of qualitative description, such as the strengths and limitations of the qualitative information, and the reasons why the information cannot be quantified.[268]

Cost-benefit analysis suggests looking at market prices to determine the monetized values of the costs and benefits of cybersecurity and network reliability. However, utilizing consumer pricing may not reflect actual costs and benefits. Using market data to inform monetization of the value of reliability and cybersecurity may be inaccurate because of the lack of

266. *Id.*
267. *Id.* at 14.
268. *See* Circular A-4, *supra* note 166, at 27.

information in the market, both to consumers and to the government. This lack of information about reliability and cybersecurity arguably means that the market for secure access is not a competitive marketplace.

Market prices are difficult to ascertain in the areas of cybersecurity and network reliability because of the interconnectedness of the network. One provider upgrading its network to increase its reliability does not affect another provider who may not be reliable, and so traffic generated by the more reliable network may nevertheless be degraded by the lack of security of other service providers. Thus, the amount of money a provider earns owing to its superior reliability might not translate into greater overall reliability. On the other hand, in the last mile market, and within each provider's network, there might be a more workable measure of reliability. The FCC must account for these factors in its analysis.

The FCC will need to evaluate the cost-effectiveness of its various regulatory options against each alternative—and against the status quo, i.e., no regulatory action. The agency must show how the proposed action will provide the anticipated costs and benefits.[269] There are a number of different options available, with varying levels of regulatory burden and reliability benefits. The least costly regulatory option is requiring reporting of network disruption events and cybersecurity problems. Because there would be no mandatory network standards or performance requirements, service providers would only bear the burden of reporting their network conditions, a matter about which they presumably already keep records. However, this option would likely have limited effectiveness and was recently considered and rejected by the FCC in the *9-1-1 Reliability Order*.[270]

While performance standards have proven successful in other regulatory contexts, such as improving fuel efficiency for vehicles,[271] their efficacy regarding network vulnerabilities is questionable. If cyber-attacks are low-probability events, it may be trivial to meet performance standards for a given year if measured in network availability uptime. In this scenario, a provider could report high performance but still not adopt the network security that is desired.[272]

An intermediate option may be certification. Regulation to require certification of the use of industry best practices or reasonable alternative measures is the approach the FCC took in the *9-1-1 Reliability Order*.[273] The order requires 9-1-1 service providers to certify their implementation

---

269. *Id.* at 18.

270. *See 911 Reliability Order*, *supra* note 192, at paras. 66-67.

271. *See generally* Greenhouse Gas Emissions Standards and Fuel Efficiency Standards for Medium- and Heavy-Duty Engines and Vehicles, EPA & NHTSA, 76 Fed. Reg. 57106 (2011).

272. This method of regulation was recently considered and rejected by the Commission in the *911 Reliability Order*. *See 911 Reliability Order*, *supra* note 192, at paras. 71-72.

273. *See 911 Reliability Order*, *supra* note 192, at paras. 44-65.

of industry best practices for reliability.[274] The FCC noted that this form of regulation "is not 'heavy-handed' or overly prescriptive, but rather flexible and designed to encourage innovation."[275] A similar tack could be taken with cybersecurity for ISPs to ensure general network reliability through consensus-based industry best practices. NIST has already laid the groundwork for this option in the Cybersecurity Framework.

The most stringent regulatory option would be to mandate specific network protocols and practices that have improved cybersecurity and reliability outcomes as compared with current practices. This is the most costly option, and its effectiveness is unclear. This may be effective for universal network protocols utilized by all service providers, such as DNSSEC and BGP discussed in Part II.A above. However, technology changes quickly, and it would probably be less cost-effective to require specific hardware and software upgrades in lieu of more flexible industry best practices than other regulatory options.[276] The Office of Management and Budget would likely oppose this method of regulation as a type of command-and-control economic regulation.

Because of inadequate information in the market, the FCC should use implicit price estimates and revealed preference measures to conduct studies to determine the value of these costs and benefits. The FCC should address industry concerns about the feasibility of a proposed regulation, but only to the extent that regulation would significantly harm the industry—i.e., by causing a large number of businesses to fail or eliminate jobs. Because of the importance of network reliability and the transition away from the PSTN to IP-based communications, the FCC should not fall into paralysis by analysis. It should act. Given the above factors and considerations, as well as the recent 911 Reliability Order, the FCC should adopt a requirement for service providers to certify implementation of industry best practices and require providers to certify compliance.

V. CONCLUSION

As more communications services become Internet-dependent, and ultimately transition to an all-IP communications system, our communications system is increasingly vulnerable to cyber-attacks. The FCC has the legal authority to implement certain measures designed to increase the cybersecurity of broadband and our nation's telecommunications infrastructure. Because of the unique threat cyber-

274. *Id.*

275. *Id.* at para. 30.

276. The FCC recognized this, and rejected tying regulations to specific technological standards in the *911 Reliability Order*. *See 911 Reliability Order*, *supra* note 192, para. 68; *see also* T. Randolph Beard, George S. Ford, Lawrence J. Spiwak & Michael Stern, *Wobbling Back to the Fire: Economic Efficiency and the Creation of a Retail Market for Set-Top Boxes*, 21 COMMLAW CONSPECTUS 1, 14 (2012).

attacks pose to our telecommunications infrastructure, including jeopardizing network reliability, interconnection, and E-9-1-1 service, potential cybersecurity regulations would be reasonably ancillary to these congressionally mandated responsibilities, and thus amenable to regulation through the FCC's ancillary authority.

The FCC should exercise this authority because the market failure in information about vulnerabilities to cyber-attacks, together with the compelling need for a reliable communications system, both justifies government regulation. The specific type of regulation adopted must carefully balance costs and benefits, and should take the form of certification of industry best practices.