

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)
)
Cyber Security Certification Program)
)
)
_____)

PS Docket No. 10-93

**COMMENTS OF
SPRINT NEXTEL CORPORATION**

Charles W. McKee
*Vice President, Government Affairs
Federal & State Regulatory*

Maria L. Cattafesta
Senior Counsel, Government Affairs

Sprint Nextel Corporation
900 7th Street, N.W., Suite 700
Washington, D.C. 20001
703-433-3786

July 12, 2010

TABLE OF CONTENTS

I.	Introduction and Summary	1
II.	Market Incentives Are Promoting Cybersecurity	3
III.	The Commission Should Consider Potential Unintended Consequences of a Certification Program	4
	A. The Certification Program Could Impede the Critical, Real-time Flexibility Necessary to Counter Cyber Threats.	4
	B. The Certification Program Could Substantially Increase the Risk that Malicious Actors Obtain and Exploit Sensitive Cybersecurity Information	7
IV.	The Commission’s Role within the Emerging Cybersecurity Framework is Unclear	8
V.	The Commission Can Take Other Important Steps to Advance Cybersecurity	10
VI.	Conclusion	13

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Cyber Security Certification Program)	PS Docket No. 10-93
)	
_____)	

**COMMENTS OF
SPRINT NEXTEL CORPORATION**

Sprint Nextel Corporation (“Sprint”) submits the following comments in response to the Federal Communication Commission’s (“FCC” or “Commission”) Notice of Inquiry (“NOI”) seeking comment on whether the Commission should establish a voluntary incentives-based cybersecurity certification program in which participating communications service providers receive FCC certification if an FCC or third party network security assessment confirms their adherence to stringent cybersecurity standards. Since market forces driving strong cybersecurity incentives currently exist, and the program could inadvertently frustrate the valuable goals it aims to achieve, Sprint respectfully suggests that the Commission continue to support CSRIC cybersecurity best practices work and develop an educational outreach program directed toward protecting the network “edge” rather than pursue the proposed certification program.

I. Introduction and Summary

The Commission seeks to establish a voluntary cybersecurity certification program to “create business incentives for providers of communication services to sustain a high level of cyber security culture and practice.”¹ Under the proposed certification program, the Commission

¹ *In the Matter of Cyber Security Certification Program*, PS Docket No. 10-93, Notice of Inquiry, 25 FCC Rcd 4345 at ¶ 1 (2010) (*NOI*).

would establish general cybersecurity objectives, which would form the basis for the development of stringent cybersecurity criteria.² Once the cybersecurity criteria are established, the Commission or a third party entity would conduct network security assessments or audits examining each provider's adherence to such standards.³ Those providers passing the security audit would receive the Commission's certification and could proceed to market its services as FCC cybersecurity compliant.⁴

While Sprint shares the Commission's valid concerns about the dangers of cyber threats, the proposed cybersecurity certification program is not the best approach to address them. A certification program is not necessary to create the powerful market incentives communications service providers already have to deploy robust cybersecurity measures to protect their networks and customers. In addition, a certification program could inadvertently impede rapid responses to emerging cyber threats and risk disclosing sensitive cybersecurity vulnerability information to hostile actors. In any event, the Commission may want to suspend consideration of a certification program until its role in the emerging federal cybersecurity landscape becomes clear, and it completes its broader broadband Notice of Inquiry.

In the meantime, Sprint suggests that the Commission continue to support the Communications Security, Reliability and Interoperability Council's ("CSRIC") cybersecurity best practices work and consider launching a cybersecurity outreach campaign to arm consumers and small businesses with the information they need to protect themselves from cyber threats. Given that the "edge" of the network creates the greatest vulnerabilities, such an educational

² *Id.* at ¶¶ 18, 28.

³ *Id.* at ¶ 28.

⁴ *Id.* at ¶¶ 51-4.

outreach program may be the most effective avenue the Commission can take to increase the overall security of the Internet.

II. Market Incentives Are Promoting Cybersecurity.

The Commission proposes to establish a cybersecurity certification program to “create a significant incentive for all providers to increase the security of their systems and improve their cyber security practices.”⁵ As a Tier 1 Internet backbone provider, Sprint believes, however, that powerful market incentives for communications service providers to adopt strong cybersecurity measures and continually refine them currently exist. Enabling a customer’s communications to flow seamlessly from one point to another is at the core of a communications service provider’s business. Cyber threats that interrupt or degrade those flows of communications can directly impair a provider’s ability to provide its core service for its customers and thus can reduce its profitability. For example, a provider that experiences a significant cyber attack that disrupts its network operations may expend substantial resources to mitigate and remediate the damage, lose customers, and repel new ones, all of which have negative financial consequences. Accordingly, communications service providers have an especially compelling economic incentive to adopt robust cybersecurity policies and practices to safeguard their networks from cyber attacks.

For Sprint, cybersecurity is an essential part of its daily operations. Sprint uses multiple mechanisms (*e.g.*, firewalls, intrusion detection and prevention systems, e-mail filtering, and anti-virus software, among other tools and practices) to protect its network from attacks in order to maintain a high level of network performance and safeguard customer traffic. In fact, Sprint employs a special dedicated team – its Computer Incident Response Team (“CIRT”) – to watch proactively for emerging threats 24 hours a day, 7 days a week and respond rapidly to incursions.

⁵ *Id.* at ¶ 13.

In addition, Sprint not only deploys cyber protections across its network, but also offers a full panoply of security solutions for business customers using Sprint's network services. For example, Sprint offers IP DefenderSM, a 24 x 7 Sprint-managed security service that monitors, alerts and mitigates Distributed Denial of Service ("DDoS") attacks before a customer's service is affected.

Sprint has developed and implemented a robust cybersecurity program, not because of a legal requirement or incentives-based program, but because the marketplace demands and expects it from Tier 1 IP Internet backbone providers, such as Sprint. Indeed, Sprint emphasizes its security efforts in an effort to differentiate itself in the market. Therefore, a Commission certification program designed to incent Sprint and other providers to adopt strong cybersecurity programs appears unnecessary. It may also prove counterproductive as set forth below.

III. The Commission Should Consider the Potential Unintended Consequences of a Certification Program.

Before developing a cybersecurity certification program, the Commission should consider the possibility that the program could inadvertently delay cyber threat responses as well as increase the risk that sensitive cybersecurity vulnerability information falls into the wrong hands.

A. The Certification Program Could Impede the Critical, Real-time Flexibility Necessary to Counter Cyber Threats.

Cybersecurity is a dynamic challenge. Cyber threats, such as DDoS attacks, botnets, and malware, including computer viruses, worms and trojans, are constantly evolving and increasing in frequency. For example, in 2009, more than 240 million distinct *new* malicious programs

were identified, which represented a 100 percent increase over 2008.⁶ Moreover, cyber attacks can quickly spiral out of control. For instance, a hostile actor can exploit security vulnerabilities using worms, which can spread with incredible propagation speed. The Slammer Worm, for example, doubled its numbers every 8.5 seconds during the first minute of its attack and was observed to infect more than 70,000 victims in ten minutes.⁷ In addition, it was estimated that the My Doom e-mail worm infected an average of one in twelve e-mail messages on the Internet at one point.⁸ As malicious actors worldwide continue to display remarkable technical ingenuity and tenacity in advancing their own cyber capabilities, cyber attacks continue to grow in speed and sophistication.

Accordingly, it is imperative that communications service providers maintain maximum flexibility to take the actions necessary to meet this dynamic challenge. As Commissioner Baker recognized, “ensur[ing] that network operators retain the flexibility and adaptability to respond to evolving cybersecurity threats” is critically important.⁹ Specifically, a provider needs the flexibility to develop, adopt and modify the tools, practices and technologies that are best suited for its particular network to keep pace with constantly evolving cyber threats. When its network

⁶ *Symantec Internet Security Threat Report, Cybercrime's Financial and Geographic Growth Shows No Slowdown during the Global Economic Crisis*, News Release, Symantec (April 20, 2010) available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf.

⁷ David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, *Sapphire/Slammer Worm Shatters Previous Speed Records For Spreading Through The Internet*, Science Daily, Feb. 5, 2003, available at <http://www.sciencedaily.com/releases/2003/02/030205073007.htm>.

⁸ Jay Munro, *My Doom.A: Fastest Spreading Virus on History*, PC Magazine, Feb. 3, 2004, available at <http://www.pcmag.com/article2/0,2817,1485719,00.asp>.

⁹ NOI at Statement of Commissioner Meredith Attwell Baker.

becomes the target of a cyber attack, it needs maximum flexibility to respond nimbly in real-time to counter, mitigate, and remediate the attack quickly and effectively.

Sprint is concerned, however, that the proposed certification program could unintentionally impede that critical flexibility and undermine communications service provider efforts to protect their networks and their customers from malicious cyber activities. In particular, the *NOI* envisions that “participating communications service providers would be assessed based on a stringent set of criteria,” possibly industry best practices.¹⁰ Imposing stringent requirements, however, could inadvertently produce detrimental results, including, but not limited to, the following:

- The certification program could lock in place certain cybersecurity practices that may subsequently become outdated. Given that cyber threats and the measures necessary to counter them are constantly changing, today’s certified measures may not necessarily be effective against tomorrow’s threats. Therefore, there is the likely danger that the required cybersecurity standards may be rendered obsolete soon after they are approved.
- Uncertainty about the scope of certified requirements could delay rapid, real-time responses to cyber threats. For example, a communications network engineer may feel the need to seek legal approval before implementing a novel cybersecurity safeguard that does not appear to fall squarely within the four corners of the certified requirements. Consequently, the program could not only delay rapid counter measure deployment, but also inhibit innovation and creativity in the process.
- The certification program could impose a “one-size-fits-all” approach when not all cybersecurity practices are appropriate for all communications service providers at all

¹⁰ *Id.* at ¶¶ 28, 32.

times. Different providers employ different types of network architectures, different technologies, and different equipment from a variety of sources. Typically, a provider develops its individual cybersecurity approach by combining methods and tools it has developed on its own with those industry best practices best suited to meet the needs of its particular network. Consequently, requiring providers to adopt practices that may not be appropriate for their unique circumstances could undermine their ability to mount the most effective cyber defense for their customers.

Therefore, a certification program imposing stringent cybersecurity requirements may not be sufficiently flexible for providers to combat continuously evolving cyber threats and thus hinder their ability to secure their networks.

B. The Certification Program Could Substantially Increase the Risk that Malicious Actors Obtain and Exploit Sensitive Cybersecurity Information.

Sprint is also concerned that the certification program could substantially increase the risk that malicious actors obtain access to and exploit highly sensitive cybersecurity information. Specifically, the program appears to involve the external collection and storage of sensitive information about individual network providers' cybersecurity practices and vulnerabilities. For example, the *NOI* proposes that providers' cybersecurity programs and related data be made publicly available.¹¹ In addition, the *NOI* asks what organization should retain the detailed results of security audits, which suggests that such data may be stored outside of the audited company.¹²

Network service providers must keep the specific details of the tools and techniques they use to combat cyber threats confidential to maintain their effectiveness. Any information made

¹¹ *Id.* at ¶ 31.

¹² *Id.* at ¶ 48.

public is available not only to consumers, but also to hostile actors looking for any leads that may help them identify and exploit potential vulnerabilities.¹³ In addition, a central repository holding information detailing the results of each network providers' individual cybersecurity audits would likely become a favorite target of cyber hackers. Accordingly, Sprint cautions the Commission that a program providing external access to detailed information about individual communications service provider cybersecurity practices will likely exacerbate cyber threats and could potentially affect national security.

IV. The Commission's Role within the Emerging Cybersecurity Framework is Unclear.

Sprint suggests that the Commission consider suspending its consideration of a cybersecurity certification program until its role in the emerging federal cybersecurity framework becomes clear. Several ongoing federal initiatives, which aim to coordinate and improve the overall cyberspace posture of the United States, could affect the Commission's activity in this area. For example, one of the near-term action items identified in the White House *Cyberspace Policy Review* is to update the national strategy to secure information and communications infrastructure.¹⁴ That updated strategy will likely inform the Commission's determination as to whether a certification program would effectively further those efforts.

In addition, federal legislation is well underway to develop a centralized, comprehensive approach to cybersecurity, which covers not only the communications sector, but the entire cyber ecosystem. Such legislation may not envision cybersecurity certification as an effective method

¹³ Even publicly identifying providers receiving certification could be problematic. Bad actors will likely surmise that those providers *not* receiving certification have lax cybersecurity standards and target them for attack.

¹⁴ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* at 37 (White House, 2009) (*Cyberspace Policy Review*).

to combat cyber threats. Even if legislation is passed requiring a similar certification approach, the authority and responsibility for implementing it may fall to another agency. For example, under the proposed *Protecting Cyberspace as a National Asset Act of 2010*, the Department of Homeland Security has the option of performing risk-based evaluations of covered critical infrastructure to determine compliance with security performance measures.¹⁵

If the Commission proceeds with the certification program, it runs the risk of implementing duplicative or conflicting regulation, which would counter its end goal of enhancing cybersecurity. As Commissioner Baker cautioned, any decisions should be “made in close coordination with other governmental efforts, particularly those of the Department of Homeland Security,” and that the Commission “should ensure our actions do not add additional layers of requirements or duplicative obligations on providers.”¹⁶ Otherwise, the resources necessary to comply with multiple, duplicative requirements would no longer be available to invest in cyber counter measures and develop new approaches to combat cyber threats.

In the meantime, whether and to what extent the Commission has a cybersecurity role under current law is unclear. As the Commission itself appears to recognize, it may not, in light of the D.C. Circuit’s recent decision in *Comcast Corp. v. FCC*,¹⁷ have the authority under the Communications Act to regulate the provision of IP-based broadband service and the facilities over which such services are provided.¹⁸ To address this uncertainty, the Commission recently

¹⁵ *Protecting Cyberspace as a National Asset Act of 2010*, S. 3480, 111th Cong. (2010) § 250; See also *Cybersecurity Act of 2010*, S. 773, 111th Cong. (2010).

¹⁶ *NOI* at Statement of Commissioner Meredith Attwell Baker.

¹⁷ *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010).

¹⁸ *NOI* at ¶¶10-11.

launched a Notice of Inquiry to examine possible legal frameworks for broadband Internet access services.¹⁹ Sprint looks forward to participating in the analysis of the Commission's jurisdiction in this broader context. The ultimate outcome of the *Broadband NOI*, however, may not give the Commission the requisite jurisdiction to establish a cybersecurity certification program. Accordingly, in light of ongoing federal initiatives to centralize and harmonize cybersecurity efforts as well as the *Broadband NOI*, Sprint suggests that the Commission suspend consideration of its certification proposal until its role and authority within the new federal cybersecurity landscape becomes clear.

V. The Commission Can Take Other Important Steps to Advance Cybersecurity.

Sprint believes that the Commission can take two important, concrete steps to advance its cybersecurity goals. *First*, Sprint suggests that the Commission continue to support and promote CSRIC's cybersecurity best practices work under its current chartered term and into the future. CSRIC is charged with providing "recommendations to the FCC to ensure optimal security, reliability and interoperability of communications systems, including telecommunications, media and public safety communications."²⁰ As part of its chartered responsibilities, CSRIC established Working Group 2A to review and update the more than 200 cybersecurity best practices that the Network Reliability and Interoperability Council ("NRIC") originally developed for the communications sector to meet today's cyber challenges.²¹

¹⁹ *In the Matter of Framework for Broadband Internet Service, Notice of Inquiry*, rel. June 17, 2010 at ¶ 2 (*Broadband NOI*).

²⁰ Charter of the FCC's Communications Security, Reliability, and Interoperability Council 1, available at http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf.

²¹ See *CSRIC Working Group Descriptions*, available at <http://www.fcc.gov/pshs/advisory/csric/wg-descriptions.pdf>. Working Group 2A -- Cyber

The NRIC/CSRIC best practices are critical to the industry because they provide communications service providers, both large and small, expert recommendations on cybersecurity practices that may be effective and feasible. In addition, the NRIC/CSRIC best practices approach offers providers the flexibility to adopt them in whole or in part as appropriate for their particular networks, systems, and processes.²² Furthermore, with the CSRIC framework already in place, voluntary best practices can be updated quicker than certified standards, which is important given that cybersecurity is a moving target requiring continual refinement. Therefore, it is important that the Commission continue to support regular updates of CSRIC cybersecurity best practices going forward to help providers keep pace with rapid advances in state of the art cybersecurity measures.

Second, Sprint proposes that the Commission explore the possibility of promoting consumer cybersecurity education and awareness. Given the interdependent nature of the Internet, cybersecurity is only as strong as its weakest link. End users are considered the most vulnerable link, and that vulnerability typically stems from lack of knowledge or awareness.²³

Security Best Practices will review cyber security best practices based on previous work under NRIC VI and VII.

²² As Focus Group 2B (Homeland Security – Cyber Security) of NRIC VII recognized, “[n]ot all Best Practices will apply to all companies nor are there Best Practices for all situations in which a company may find a cyber security problem.” *Summary of Activities, Guidance and Cybersecurity Issues*, Focus Group 2B, available at http://www.nric.org/meetings/docs/meeting_20051216/FG2B_Dec%2005_Final%20Report.pdf.

²³ See *State of the Web – Q4 2009, A View of the Web from an End User’s Perspective*, Zscaler Labs at 19, available at http://www.zscaler.com/pdf/industryreports/state_of_the_web_q4_2009_noapp.pdf.

End-users need information on how to protect themselves from cyber threats, such as web-based malware, social engineering schemes, and virus attacks.²⁴

The Commission is well positioned to launch a cybersecurity public awareness campaign targeting consumers and small businesses, given its experience in communicating technical advice to the public in a clear, understandable way using multiple forms of media. The Commission's DTV transition education campaign is an excellent example of a comprehensive campaign to help guide consumers through a thicket of advanced technical information and provide them direction. More recently, the Commission's *Wireless World Travel Week* offered travelers important money-saving tips on international wireless service, using the Commission's "Savvy Traveler" blog posts and Twitter page, a video, and a tip sheet for consumers.²⁵

In a cybersecurity awareness campaign, the Commission, using multiple forms of media, could educate end users about the various types of threats, how to protect themselves from such threats (*e.g.*, password management, installing and maintaining anti-virus software and firewalls, using caution with e-mail attachments, avoiding phishing scams), and the steps to take if they become victims of a cyber intrusion. Combining the expertise of both the Public Safety and Homeland Security Bureau and the Consumer and Government Affairs Bureau should produce an effective outreach program to help arm consumers and small businesses with the knowledge they need to combat cyber threats.

²⁴ As the President's *Cyberspace Policy Review* notes, "[p]eople cannot value security without first understanding how much is at risk." *Cyberspace Policy Review* at iv.

²⁵ *FCC Announces Wireless World Travel Week; FCC and Wireless Providers Offer Money-Saving Calling Tips for Foreign Travel*, News Release, rel. June 21, 2010.

VI. Conclusion

For the foregoing reasons, Sprint respectfully suggests that the Commission suspend its consideration of its proposed cybersecurity certification program. Instead, the Commission should continue to support CSRIC cybersecurity best practices work and explore launching a cybersecurity education and awareness program for consumers and small businesses to help advance its policy objectives.

Respectfully submitted,

SPRINT NEXTEL CORPORATION

/s/ Charles W. McKee _____
Charles W. McKee
*Vice President, Government Affairs
Federal & State Regulatory*

Maria L. Cattafesta
Senior Counsel, Government Affairs

Sprint Nextel Corporation
900 7th Street, N.W., Suite 700
Washington, D.C. 20001
703-433-3786

July 12, 2010