

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
FCC Seeks Public Comment on National)	PS Docket No. 10-146
Broadband Plan Recommendation to Create a)	GN Docket No. 09-51
Cybersecurity Roadmap)	
)	

COMMENTS OF CTIA—The Wireless Association®

Michael F. Altschul
Senior Vice President and General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Brian M. Josef
Director, Regulatory Affairs

CTIA—The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

September 23, 2010

EXECUTIVE SUMMARY

Ensuring effective security of customers' data and communications is of paramount importance to the wireless industry and will become increasingly important as Americans continue to find new ways of integrating wireless broadband technologies into their daily lives. While CTIA shares the Commission's goal of strengthening cyber security protections of today's communications networks and applauds the Commission's recent focus on this issue, CTIA has serious concerns about the proposed Cyber Security Roadmap, which could inadvertently weaken cyber security efforts.

Although well intentioned, the Commission's proposed Cyber Security Roadmap is troubling because of its potential to actually make wireless networks less secure. By providing details of the vulnerabilities of commercial broadband networks and the steps planned by the public and private sectors to address these vulnerabilities, the roadmap runs the serious risk of becoming a tool for cyber attacks. Moreover, by setting forth a specific path to cyber security, along with clearly defined milestones and benchmarks, the Cyber Security Roadmap threatens to reduce the flexibility required by wireless network operators to dynamically manage their networks and thus hamstring their cyber security efforts.

Rather than pursuing the proposed Cyber Security Roadmap, CTIA respectfully submits that the Commission should look for other, potentially more beneficial opportunities to contribute in this area. For example, the Commission may be able to most effectively promote cyber security efforts through consumer education and outreach, which could dramatically reduce the number of cyber threats that reach commercial broadband networks. Furthermore, the Commission should be mindful of the myriad efforts already underway in other branches of the government and it should attempt to contribute meaningfully to these initiatives. Ultimately, an

effective cyber security regime may require national coordination, and the Commission should take pains to ensure that its efforts complement, rather than complicate, such developments.

Due to fierce competition in the wireless market, cyber security has become an essential aspect of the network management activities of all wireless providers. In an industry characterized by high consumer turnover, network operators cannot afford to provide anything less than the best when it comes to security. As a result of these powerful market incentives, the wireless industry has been a leader in voluntary efforts to design and implement cyber security best practices and to educate consumers about how to identify and avoid risky behaviors online. In addition to the participation by wireless industry members in numerous public and private sector cyber security initiatives, this commitment to cyber security is demonstrated by the wireless industry's strong record of preventing and mitigating cyber attacks.

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	i
I. INTRODUCTION	1
II. THE WIRELESS INDUSTRY CONTINUES TO EFFECTIVELY ESTABLISH AND PROMOTE CYBER SECURITY INITIATIVES	2
A. Voluntary Industry Efforts Have Been Largely Successful in Establishing Practices and Techniques for Protecting Wireless Networks	3
B. Through Competition, the Wireless Marketplace Creates Incentives for Cyber Security.	5
III. THE COMMISSION, IN CONTEMPLATING A CYBER SECURITY ROADMAP, SHOULD BE WARY OF THE FAST-PACED NATURE OF CYBER THREATS	7
A. The Commission’s Cyber Security Roadmap Must Not Provide a List of Our Most Vulnerable Networks to Potential Cyber Criminals	8
B. Carriers Must Retain Their Ability to Utilize Reasonable Network Management Techniques to Guard Against Cyber Threats.	9
IV. ANY CYBER SECURITY EFFORTS UNDERTAKEN BY THE FCC SHOULD BE COORDINATED WITH OTHER BRANCHES OF GOVERNMENT	11
V. CONCLUSION.....	14

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
FCC Seeks Public Comment on National) PS Docket No. 10-146
Broadband Plan Recommendation to Create a) GN Docket No. 09-51
Cybersecurity Roadmap)
)

COMMENTS OF CTIA—The Wireless Association®

CTIA—The Wireless Association® (“CTIA”)¹ respectfully submits the following comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) Public Notice seeking comment on the creation of a Cyber Security Roadmap to identify vulnerabilities of communications networks or threats to end-users.²

I. INTRODUCTION

The wireless industry shares the Commission’s concern over the serious threat posed by cyber attacks and understands the importance of secure broadband networks to our society, economy, and national defense. Although the industry shares the Commission’s goal of ensuring the most secure broadband experience possible, it cautions the Commission that the cyber security roadmap contemplated may not be well-suited to the constantly changing nature of cyber threats as well as network operators’ needs for significant flexibility in reasonably

¹ CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service (“CMRS”) providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

² *FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap*, PS Docket No. 10-146, GN Docket No. 09-51, Public Notice, DA 10-1354 (rel. Aug. 9, 2010) (“Public Notice”).

managing their networks. Rather than moving forward with the Cyber Security Roadmap proposal, which could inadvertently hinder effective cyber security, CTIA urges the Commission to consider how it can coordinate its efforts and resources with initiatives already underway or contemplated by other government bodies and the private sector.

The wireless industry has long engaged in successful voluntary security efforts because it recognizes that cyber security is a competitive imperative. Indeed, market incentives have driven the industry to incorporate dynamic cyber security protections as an essential part of the network management constantly engaged in by wireless providers. As detailed below and in previous filings,³ the wireless industry is a leader in providing effective security safeguards and outreach programs designed to protect its consumers and their data.

II. THE WIRELESS INDUSTRY CONTINUES TO EFFECTIVELY ESTABLISH AND PROMOTE CYBER SECURITY INITIATIVES.

Cyber crime is nothing new to the wireless industry. Since the days of cell phone cloning, the members of the wireless industry have had a long and successful track record of combating cyber crime and threats. The industry's success in this regard is the product of diligent network management coupled with the implementation of best practices and security techniques developed and promulgated through voluntary coordination. In the highly competitive wireless marketplace, network operators cannot and do not take security for granted. Consumers who feel that their data and communications are unsecure will not hesitate to change service providers. This competitive environment fosters incentives for innovation and excellence in cyber security that no government-established regulatory program can match.

³ See Comments of CTIA—The Wireless Association®, GN Docket Nos. 09-47, 09-51, 09-137 (filed Nov. 12, 2009); Comments of CTIA—The Wireless Association®, PS Docket No. 10-93 (filed July 12, 2010); Comments of CTIA—The Wireless Association®, Dept. of Commerce Docket No. 100402174-0175-01 (filed Sept. 20, 2010).

A. Voluntary Industry Efforts Have Been Largely Successful in Establishing Practices and Techniques for Protecting Wireless Networks.

The success of the wireless industry's cyber security practices is best evidenced by the relative lack of major exploits of cyber vulnerabilities on wireless broadband networks to date. When security breaches have occurred, they have largely been addressed quickly, effectively, and transparently. Yet, the wireless industry is not resting on its laurels. Efforts to develop and implement improved cyber security best practices have been ongoing for years within the industry, and continue in earnest. These voluntary efforts help ensure that wireless network operators continue to innovate and evolve their cyber security offerings to prevent and respond to the incursion of the ever-changing cyber threat.

CTIA, as the premier trade association for the wireless industry, has taken a leadership role in organizing industry participation in security-related collaborations. Over the past 15 years, CTIA has administered a variety of programs that deal with different aspects of network security. Wireless carriers manage and maintain the largest private key security systems in the world, and when they established these systems to prevent access fraud in the 1990s, they underwent extensive security audits, then developed the systems, programs and security culture required to secure these keys and other valuable data stored in their networks from disclosure and attack. Carriers developed and shared best practices on password security, access controls, and life-cycle management of security keys. They were early adopters of new and evolving technologies including multi-token authentication credentials, advanced firewalls, intrusion detection systems, and "push" software patching. For over a decade, CTIA has convened a monthly meeting that discusses trends attackers are using in their attempts to steal service, illegally access data, or use social engineering to trick customers or employees. The group

reports on suspicious activities and successful strategies to combat these attacks with their carrier counterparts.

Additionally, CTIA has convened a Cyber Security Working Group comprised of members to address key areas of concern in this area. CTIA also has designed and administered a Business Continuity/Disaster Recovery program that certifies industry members' response plans in the case of critical service interruptions, including in the case of a large-scale cyber attack. The main elements of this program are detailed in an attachment to this filing.⁴ Through this program, wireless service providers have integrated cyber security planning into their business practices, assessing potential risks and developing appropriate responses. The wireless industry also has the benefit of detailed best practices that can be customized for each service provider's particular circumstances. For example, the industry participated actively in the work of the Commission's Network Reliability and Interoperability Council ("NRIC"), which issued over 200 recommendations pertaining to cyber security.⁵ Furthermore, last year the Commission re-chartered the council as the Communications Security, Reliability, and Interoperability Council ("CSRIC"), which, among other tasks, is reviewing and supplementing the NRIC recommendations to ensure that a set of effective and relevant cyber security best practices are available to all. CTIA and several wireless industry members are actively collaborating with the CSRIC, including members with representation on the CSRIC Working Group 2A dedicated to reviewing the cyber security best practices.

The wireless industry partners with dozens of federal and local governmental agencies and nonprofit organizations to address various aspects of cyber security and network reliability.

⁴ See Attachment 1.

⁵ See "NRIC Best Practices" <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm> (last visited Sept. 10, 2010).

This participation ranges from assisting the Department of Homeland Security in developing the National Infrastructure Protection Plan (“NIPP”), to working closely with the National Communications System (“NCS”) and the United States Computer Emergency Readiness Team (“US-CERT”) to share information regarding unusual activities and to fortify communications networks. Industry members also are significant contributors to direct consumer education campaigns such as the National Center for Missing and Exploited Children’s NetSmartz.org, the National Cybersecurity Alliance’s StaySafeOnline.org portals and ConnectSafely.org. These voluntary efforts have resulted in the development of a broad array of strategies, partnerships, and best practices that work together to ensure, to the greatest extent possible, the security of wireless broadband networks.

CTIA also educates children and teens on maintaining a safe Internet experience through the “Be Smart. Be Fair. Be Safe: Wireless Responsible Use” campaign, as well as complementary initiatives with entities such as Common Sense Media and the Illinois Attorney General’s Office. The campaign aims to equip parents and teachers with tools to teach kids about responsible mobile device use, including behavior that could lead to misuse or abuse of a mobile device and user information.⁶

B. Through Competition, the Wireless Marketplace Creates Incentives for Cyber Security.

The wireless industry has effectively embraced the need to ensure cyber security because of the substantial market incentives that foster a culture of innovation and investment. In every aspect of the dynamic wireless ecosystem, competition fuels research and development. It also fuels the need to protect consumers. From the development of cutting-edge devices to the

⁶ See <http://www.besmartwireless.com/>.

provision of reliable service, the wireless industry ecosystem continually strives to deliver a superior product that serves customer demands and interests.

As a result, cyber security is a core aspect of the network management activities of all wireless service providers. Service providers have extensive market incentives to invest in state-of-the-art cyber security measures. Indeed, these service providers recognize that cyber security is a competitive necessity in today's broadband marketplace. With approximately 25% subscriber churn in 2009,⁷ network operators compete on every available playing field. In addition to price, network coverage, and devices, reliability and quality of service are key considerations for wireless network operators as they strive to attract and retain subscribers. These market realities create effective incentives for wireless network operators to take cyber security seriously and to constantly stay ahead of the curve—more than any regulatory initiative or government program could hope to accomplish.

Cyber security threats such as spam, viruses, and botnets have the potential to affect wireless networks through unwanted network traffic and malicious code that could damage the network, endanger subscriber data, or otherwise diminish the broadband user experience. Because they are so rare, major wireless broadband security breaches receive significant attention. True mobile broadband is nascent, with carriers providing Third Generation (“3G”) services that are competitive with wireline broadband services in many portions of the country and beginning to deploy Fourth Generation (“4G”) wireless broadband services that will, for the first time, replicate (and in some cases surpass) the broadband speeds and experience that many users enjoy on traditional wireline home broadband networks. It is essential that users trust the

⁷ Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, including Commercial Mobile Radio Services, WT Docket No. 09-66, *Fourteenth Report*, FCC 10-81 at 9-10 (rel. May 20, 2010).

security of their personal information if adoption of next generation wireless broadband networks is to flourish and if carriers are to see a return on their substantial investments.

Unless service providers actively anticipate and respond to cyber security threats, consumer confidence in those providers will wane, leading to a loss of subscribership and revenue. As such, ensuring network security is extremely vital for wireless network operators, and these activities have become standard components of the services provided. For example, one form of network management that consumers have come to expect and embrace is spam blocking, which wireless carriers provide for both email and text messaging.⁸ However, service providers are constantly engaged in a variety of other proactive safeguards, such as monitoring traffic patterns from known origins of malicious code, and tracking the greater trends and flows on the network ports themselves. These transparent activities, largely provided to subscribers without additional charge, effectively prevent many cyber threats from ever reaching wireless consumers.

III. THE COMMISSION, IN CONTEMPLATING A CYBER SECURITY ROADMAP, SHOULD BE WARY OF THE FAST-PACED NATURE OF CYBER THREATS.

The greatest challenge in cyber security is that the threats often change more quickly than the techniques used to combat them. Wireless network operators must be prepared for countless varieties of attack. Under these conditions, wireless service providers and other commercial entities require the flexibility to be innovative and dynamic in their responses to cyber threats. CTIA has reservations about the proposal to draft a roadmap of “the five most critical cyber security threats to the communications infrastructure” because of the potential for that roadmap

⁸ See, e.g., *More Good News for Wireless Consumers*, Blog Post of Christopher Guttman-McCabe, Aug 31, 2010 (noting that, despite carriers’ aggressive efforts to protect against spam, stronger regulatory enforcement to combat and deter these third party violations of the TCPA and CAN-SPAM Act is necessary), available at <http://www.ctia.org/blog/index.cfm/2010/8/31/More-Good-News-For-Wireless-Consumers>.

to be used by cyber criminals in perpetrating even more effective attacks. Moreover, as the Commission examines the appropriate role for it in “address[ing] vulnerabilities to core Internet protocols and technologies”⁹ it should be mindful of the risk that any government-established fixed standards or practices likely would soon be outdated by the swift development of cyber threats and could result in increased vulnerability rather than an effective safeguard.

A. The Commission’s Cyber Security Roadmap Must Not Provide a List of The Most Vulnerable Networks to Potential Cyber Criminals

As discussed above, CTIA is an active participant in several ongoing cyber security initiatives and strongly supports all efforts to bolster networks and infrastructure against cyber threats. Thus, CTIA fully understands the importance of recognizing critical vulnerabilities in commercial networks and developing strategies and solutions for strengthening them. However, because of the public participation and transparency that are requirements and hallmarks of its policymaking, the Commission is likely not the best forum in which to conduct these sensitive deliberations.¹⁰

The Public Notice outlines a process through which the Commission would “identify the five most critical cyber security threats to the communications infrastructure and its end users and establish a two-year plan, including milestones, for the FCC to address these threats.”¹¹ Despite the potential utility of such a process, a detailed list of vulnerabilities provided by network operators and other wireless industry participants would be equally or more useful to

⁹ Public Notice at 1.

¹⁰ CTIA recognizes that the parties may seek confidential treatment for their submissions to the Commission, however, it notes that this was not emphasized in the Public Notice and the Commission is regularly asked to make public certain sensitive carrier information through Freedom of Information Act requests or other administrative or judicial processes.

¹¹ Public Notice at 1 (*citing* Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: The National Broadband Plan* (March 2010) at 123 (Recommendation § 16.5)).

those who would seek to harm wireless networks. Furthermore, by publicizing not only the network vulnerabilities, but also the details and schedule for addressing these vulnerabilities, the cyber security roadmap may provide for cyber attackers a guide on how to circumvent the ongoing security improvements of the communications industry. Although CTIA wholeheartedly endorses the excellent best practices development work being done by bodies such as the CSRIC, the Commission should avoid collecting and publishing detailed information about the cyber security vulnerabilities of proprietary wireless networks.

B. Carriers Must Retain Their Ability to Utilize Reasonable Network Management Techniques to Guard Against Cyber Threats.

The Commission should avoid prescriptively regulating network operator cyber security practices through this or any other proceeding. The time and compromises inevitable in agency processes of setting government standards risk the obsolescence of those standards and may not facilitate the needed nimble, rapid response and development of new protective cyber security measures. Proactive thinking and dynamic protections are necessary to guard against the evolving cyber threat. Yet, service providers and other commercial entities may be forced to direct resources towards abiding by government-set standards that may hamstring other, more effective initiatives. Equally troubling is the potential for any government-mandated cyber security standards to provide a roadmap to the defenses and vulnerabilities of commercial enterprises that could be exploited by would-be cyber attackers. The need for flexibility is particularly acute in the mobile context, where network operators have unique concerns imposed by the temporal and geographic nature of network use in a spectrally-constrained environment. Rather than expending valuable government and private sector resources on developing standards that are likely to be at least partly irrelevant before they are completed, the Commission should identify more effective opportunities to improve overall cyber security.

Despite the best efforts of service providers, complete protection from every potential cyber threat is not possible. Vulnerabilities exist by virtue of risky user behavior and third party behavior outside the control of wireless service providers. For example, smartphones increasingly include Wi-Fi connectivity that offers users the ability to connect to the Internet wirelessly without utilizing licensed commercial carriers' spectrum. However, when users choose to connect over unsecured third party wireless networks, commercial wireless service providers have no visibility into or control over the network traffic to which users are exposed. Similarly, the open nature of the Internet, the explosion of applications, and the introduction of multiple app stores mean that users often have access to third party applications that may contain hidden vulnerabilities or might even be masks for malicious code. In these and many other cases, cyber attacks are preventable if users take appropriate precautions.

Ultimately, the best defense, as a supplement to reasonable dynamic network management, is to educate wireless consumers to the greatest extent possible about new threats and safe network usage. CTIA and its member companies actively engage in such consumer education campaigns,¹² and this is an area worthy of further investigation to determine the role the Commission and other governmental bodies could play. As wireless industry members have indicated in previous cyber security-related proceedings, the Commission has a demonstrated ability to plan and execute successful consumer education campaigns.¹³ It is possible that the Commission's resources might be best marshaled towards exercising these skills in conjunction with other established consumer outreach efforts.

¹² See, e.g., Comments of AT&T, Inc., GN Docket Nos. 09-47, 09-51, 09-137 at 40-41 (filed Nov. 12, 2009) (discussing internal programs and external partnerships); Connect Safely, <http://www.connectsafely.org/>; NetSmartz.org, <http://www.netsmartz.org/>; StaySafeOnline.org, <http://www.staysafeonline.org/>.

¹³ See Comments of AT&T, Inc., PS Docket No. 10-93 at 26-27 (filed July 12, 2010); Comments of Sprint Nextel Corporation, PS Docket No. 10-93 at 11-12 (filed July 12, 2010).

IV. ANY CYBER SECURITY EFFORTS UNDERTAKEN BY THE FCC SHOULD BE COORDINATED WITH OTHER BRANCHES OF GOVERNMENT.

The Commission must ensure that any cyber security initiative it launches is closely coordinated with existing efforts within the federal government, so as to most efficiently use resources and to achieve optimal results. Cyber security is recognized as a significant and essential challenge across the public and private sectors. Additionally, because of its far-reaching impact on everything from the economy to national defense, cyber security touches on the jurisdiction of countless arms of the government. Indeed, there are literally scores of federal and local agencies engaged in significant cyber security actions. To illustrate, a recent inquiry identified more than 55 government-initiated, public-private partnerships addressing cyber security—with over 30 based out of the Department of Homeland Security (“DHS”) alone.¹⁴ The list of executive branch agencies that address worms, viruses, hacking, Denial of Service attacks, and other cyber security vulnerabilities includes (but is not limited to):

- Within DHS: the National Cyber Security Division, US-CERT, and NCS;
- Within the Department of Justice: the Federal Bureau of Investigation, and the Computer Crime and Intellectual Property Section;
- Within the Department of Defense: the Defense Information Systems Agency, the National Security Agency, the Defense Advanced Research Projects Agency, and the cyber security units within each branch of the military;
- Within the Department of Commerce: the National Institute for Standards and Technology, the National Telecommunications and Information Administration, and the International Trade Administration; and
- Within the White House: the Office of Science and Technology Policy and the National Cybersecurity Coordinator.

¹⁴ See Melissa Hathaway, “Why Successful Partnerships are Critical for Promotion Cybersecurity” <http://www.thenewnewinternet.com/2010/05/07/why-successful-partnerships-are-critical-for-promoting-cybersecurity/> (May 7, 2010).

Congress has taken up these issues as well. Multiple pieces of legislation currently before the U.S. Congress propose creating various cyber security offices, directorships, and varying responsibilities for numerous federal government agencies, including, in some cases, a Senate-confirmed office within the Executive Office of the President with virtually plenary supervisory authority over all Federal cyber security initiatives.¹⁵ Indeed, both the Rockefeller-Snowe and the Lieberman bills include mechanisms by which key industry members would share information with the government in an attempt to identify vulnerabilities and develop best practices. In some cases, these bills provide important liability and confidentiality protections for participating industry members that are not contemplated in the Commission's proposal.

Perhaps unsurprisingly, a common complaint about the government's approach to cyber security is that it is overly balkanized and uncoordinated, with various agencies performing duplicative or even conflicting actions. To illustrate, the Government Accountability Office recently released an analysis of the cyber security research and development ("R&D") initiatives being pursued by the Federal government.¹⁶ Ultimately, the report concludes that, although steps to coordinate the various cyber security R&D programs have been taken, significant challenges still exist that demand strong central coordination. "Specifically, the absence of a national cyber security R&D agenda and leadership increases the risk that efforts will not reflect national

¹⁵ See Cybersecurity Act of 2009, S. 772, 111th Cong. (2009) ("Rockefeller-Snowe"); A Bill to Establish, Within the Executive Office of the President, the National Cybersecurity Advisor, S. 778, 111th Cong. (2009); Protecting Cyberspace as a National Asset Act, S. 3480, 111th Cong. (2010) ("Lieberman").

¹⁶ See Government Accountability Office, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development*, GAP-10-466 (June 2010) available at <http://www.gao.gov/new.items/d10466.pdf>.

priorities, key decisions will be postponed and federal agencies will lack overall direction for their efforts.”¹⁷

In light of this uncertainty, it is not clear that the Commission is an appropriate agency to launch a new cyber security initiative or to attempt to manage the existing efforts. However, the Commission does have key expertise and experience related to the communications industries that could be valuable when contributed to some of these ongoing efforts. To ensure that the most effective cyber security programs are crafted, CTIA urges the Commission to consider how its efforts to prevent or minimize cyber threats can be coordinated with those already ongoing in other agencies. Ultimately, the worst thing for consumers at this time would be a disorganized and uncoordinated effort that splits the attention and resources of the industry, thereby undermining the efficacy of all cyber security efforts.

¹⁷ *Id.* at 21.

V. CONCLUSION

The wireless industry appreciates the crucial importance of addressing the nation's cyber security vulnerabilities and applauds the Commission's recent attention to this matter. The industry has long recognized that providing effective cyber security is essential to remaining competitive in the wireless marketplace. To succeed in this effort, wireless providers require continued flexibility to dynamically manage and protect their networks. CTIA has serious concerns about the Commission's proposed Cyber Security Roadmap, the questionable benefits of which appear to be outweighed by its potentially negative consequences. CTIA respectfully urges the Commission, in pursuing its cyber security goals, to focus on alternative approaches, such as consumer education and outreach, and most importantly to ensure the coordination of its efforts with cyber security initiatives ongoing elsewhere in the public and private sectors.

Respectfully submitted,

By: /s/ Brian M. Josef
Brian M. Josef
Director, Regulatory Affairs

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President and General Counsel

CTIA—The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

September 23, 2010

Attachment 1

**ELEMENTS OF CTIA – THE WIRELESS
ASSOCIATION’S VOLUNTARY BUSINESS
CONTINUITY / DISASTER RECOVERY PROGRAM**

ELEMENTS OF CTIA – THE WIRELESS ASSOCIATION’S VOLUNTARY BUSINESS CONTINUITY / DISASTER RECOVERY PROGRAM

Requirement 1: Project Initiation and Management

Companies must demonstrate that they have done the following:

Defined objectives

Developed project plan and budget

Defined and recommended process structure and management

Obtained senior management commitment

Requirement 2: Risk Evaluation and Control

Companies must demonstrate that they have done the following:

Identified risks, events, and external surroundings that can adversely affect the company

Evaluated the damage that such risks and events could cause and probability of occurrence

Identified controls and safeguards to prevent or mitigate losses to company

Requirement 3: Business Impact Analysis

Companies must demonstrate that they have done the following:

Identified the critical functions of the organization

Identified the impacts resulting from disruptions and disaster scenarios

Determined recovery priorities and timeline objectives

Requirement 4: Developing Business Continuity Strategies

Companies must demonstrate that they have done the following:

Selected business recovery operating strategies

Assessed risk associated with each optional continuity strategy

Requirement 5: Emergency Response and Operations

Companies must demonstrate that they have done the following:

Developed and implemented procedures for response to situations

Established a process for activation of an Emergency Operations Center

Integrated Disaster Recovery/Business Continuity procedures with Emergency Response procedures

Established Command and Control procedures

Requirement 6: Developing and Implementing Business Continuity Plans

Companies must demonstrate that they have done the following:

Established and implemented Business Continuity and Crisis Management plans

Established procedures to transition from emergency response to crisis management / business continuity

Established a procedure to maintain and update Business Continuity plans

Requirement 7: Awareness and Training Programs

Companies must demonstrate that they have done the following:

Established a process to educate the company regarding business continuity issues and programs

Developed and presented training programs

Requirement 8: Exercise Business Continuity Program

Companies must demonstrate that they have done the following:

Established a process to drill/exercise the Business Continuity / Disaster Recovery program

Organized and completed exercises/drills

Developed and monitored after-action reports and results of exercises

Requirement 9: Public Relations and Crisis Coordination

Companies must demonstrate that they have done the following:

Developed plans to communicate with employees and management

Developed process to communicate, if necessary, with other stakeholders

Requirement 10: Coordination With External Agencies

Companies must demonstrate that they have done the following:

Established applicable procedures and policies for coordinating response with government representatives

Source: Copyright 2004 DRI International – Reprinted with Permission