

ATT Wireless.txt
Subject: Comments of AT&T Wireless Services, Inc.
Date: Mon, 16 Jun 2003 14:58:32 -0400
From: "Krinsky, Adam" <AKrinsky@wbklaw.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attached please find the comments of AT&T Wireless Services, Inc. submitted in response to the Department of Homeland Security's Critical Infrastructure Information Notice of Proposed Rulemaking.

Please confirm receipt of these comments. If you have any problems opening the file, please contact me.

Regards,
Adam Krinsky

Adam D. Krinsky
Wilkinson Barker Knauer, LLP
2300 N Street, NW Suite 700
Washington, DC 20037
(tel.) 202.383.3340
(fax) 202.783.5851
akrinsky@wbklaw.com

AWS 061603 DHS Comments.pdf Name: AWS 061603 DHS Comments.pdf
Type: Acrobat (application/pdf)
Encoding: base64
Description: AWS 061603 DHS Comments.pdf

In the Matter of)
)
 Procedures for Handling Critical Infrastructure)
 Information)
)

AT&T Wireless Services, Inc. (“AT&T Wireless”) respectfully submits these comments in response to the Notice of Proposed Rulemaking (“*Notice*”) in the above-captioned proceeding.¹

I. BACKGROUND AND SUMMARY

AT&T Wireless is a publicly traded company (NYSE: AWE) which split off from AT&T Corp. in July 2001 to become the largest independently owned and operated wireless company in North America. Now entirely dedicated to wireless communications, AT&T Wireless serves more than 21 million subscribers. Customers include individual subscribers, small-, medium-, and large-sized enterprises, and public safety organizations. AT&T Wireless offers a wide variety of wireless services, including: voice and text messaging services; e-mail functionality; multimedia messaging combining pictures, sounds and text; Internet access; enterprise solutions; and Wi-Fi capability. The company's wireless systems have a coverage footprint that reaches more than 74 percent of the U.S. population and an overall service area, including roaming

¹ *Procedures for Handling Critical Infrastructure Information*, Notice of Proposed Rulemaking, 68 Fed. Reg.18524 (2003) (to be codified at 6 C.F.R. pt. 29) (proposed Apr. 15, 2003) (“*Notice*”).

capabilities, that covers virtually the entire U.S. population. With regard to international service, AT&T Wireless customers can place calls to over 220 countries. When abroad, customers can make voice calls from over 100 countries on 6 continents. In fact, customers can use an AT&T Wireless phone in more countries than any single handset from any other U.S. carrier. AT&T Wireless has received *Business Traveler Magazine*'s "Best in Business Travel" Reader Survey Awards as the number one mobile phone service provider and the best international wireless service.

The telecommunications industry has a long record of collaboration with federal, state, and local governments in working to ensure the reliability and security of the telecommunications infrastructure. Historically, these efforts have focused on preparing for and responding to natural disasters including tornadoes, hurricanes and floods, dealing with accidents such as unintentional cable cuts, and safeguarding the general dependability of public telecommunications networks. The recent emergence of terrorism and sabotage has heightened the national interest in the physical and cyber security of the country's communications networks. Given this new threat environment, the importance of public-private collaboration and information sharing regarding vulnerabilities, prevention, and restoration has never been greater. AT&T Wireless, therefore, supports the Department of Homeland Security's ("DHS") proposal to protect critical infrastructure information, pursuant to the Critical Infrastructure Information Act of 2002 ("CII Act"), adopted as subtitle B of Title 2 of the Homeland Security Act.² Sound implementation of the CII Act will foster an environment conducive to sharing information about vulnerabilities, potential or actual attacks, and the ability to resist or recover from any such

² Homeland Security Act, Pub. L. No. 107-296, §§ 212-215, 116 Stat. 2135, 2150-2155 (2002).

event. Together, industry and government can work to reduce the risks to our nation's communications networks.

AT&T Wireless views the responsibilities of corporate citizenship seriously and demonstrates its commitment to national security, law enforcement, and public safety in many different ways. The company, for example, is a member of the Network Reliability and Interoperability Council ("NRIC"), a Federal Advisory Committee chartered by the Federal Communications Commission ("FCC"). NRIC is charged with identifying industry Best Practices to address external threats to communications infrastructure, among other things. NRIC has established Focus Groups to address several aspects of Homeland Security, including Physical Security, Cyber Security, Public Safety, and Disaster Recovery and Mutual Aid. AT&T Wireless has actively participated in several Focus Groups to help address homeland security issues.

AT&T Wireless also works closely with federal, state, and local law enforcement to fulfill its responsibilities under the Communications Assistance for Law Enforcement Act ("CALEA") and the USA PATRIOT Act. These responsibilities include the deployment of law enforcement intercept capabilities and the implementation of wiretaps pursuant to judicial process.

With regard to public safety, AT&T Wireless has embarked on an aggressive E-911 deployment plan to provide public safety communications officials with the call-back number and location coordinates of wireless 911 callers. The FCC has noted that wireless callers place from 30-50 percent of all 911 calls, and AT&T Wireless is committed to doing its part to provide public safety communications officials with information that can aid law enforcement and public safety personnel in assisting citizens in need.

AT&T Wireless is also in discussions with the National Communications System, a part of DHS's Information Analysis and Infrastructure Protection Directorate, about the provision of Wireless Priority Service for National Security/Emergency Preparedness ("NS/EP") personnel.

II. THE SEPTEMBER 11 EXPERIENCE: THE IMPORTANCE OF WIRELESS SERVICE, DISASTER PREPAREDNESS, AND COLLABORATIVE EFFORTS

In the last several years, wireless communications services have become a vital thread in the fabric of American life. Parents are able to stay in touch with their children. Friends can make last-minute plans whenever they are "on the go." An increasingly mobile workforce can connect back to the office – whether across the street or across the globe. Wireless service is also a vital asset for ordinary citizens and emergency personnel in a time of crisis. This lesson was never more evident than on September 11, 2001.

The tragic events of September 11 made abundantly clear that wireless communications are crucial to the ability of law enforcement, public safety, and affected citizens to communicate during a disaster. Wireless service made it possible for people trapped in buildings to call for help and, in some cases, to call their loved ones for one last time. It enabled passengers on a plane likely bound for the White House or the Capitol to obtain information in time to take heroic action and avert an even larger disaster. Wireless service allowed residents of New York, Washington, D.C., and across the nation to let their children, parents, spouses, and friends know they were safe. Wireless service – including commercial operations – was also essential for firefighters, police, and other emergency first responders in those cities to coordinate their rescue efforts, and for utility workers to coordinate their repair and salvage efforts.

Although the attacks did not directly target the telecommunications infrastructure, they put enormous strain on our nation's telecommunications networks. Systems in New York City,

in particular, suffered significant damage, including AT&T Wireless systems.³ Yet AT&T Wireless and other telecommunications providers responded to the challenge.

Just minutes after the first plane struck the World Trade Center complex, AT&T Wireless activated its highest level of disaster response – its National Emergency Operations Center – to coordinate efforts at the national, regional, and local levels and to identify all available personnel and equipment to support recovery and repair activities. The company brought in 26 technicians from other markets, who helped devise alternate ways to provide service in areas around impaired cell sites. The company obtained special temporary authorization from the FCC to gain access to 10 MHz of unused spectrum licensed to NextWave in the New York market to increase the network’s maximum capacity. All told, AT&T Wireless activated 17 “Cells on Wheels,” or “COWs”: 15 in New York, one in Washington, D.C., and one in Pennsylvania. In addition, the company deployed 12 portable generators to support the cell sites that had lost commercial power.

While AT&T Wireless’s primary focus in the immediate aftermath of September 11 was to avert a network disaster and to maintain much needed wireless service to public safety and commercial users, it also supported the ongoing search and recovery efforts at Ground Zero and the Pentagon. Together with several other telecommunications companies, AT&T Wireless participated in the Wireless Emergency Response Team (“WERT”) to assist emergency response personnel in searching for possible survivors in the World Trade Center rubble. Tragically, no trapped survivors were found, but the WERT response demonstrated that a coordinated wireless

³ Forty-seven AT&T Wireless cell sites were knocked out of service, one cell site was destroyed, Verizon’s major switching office across the street from the World Trade Center was destroyed, all of lower Manhattan sustained a complete commercial power failure, and wireless call volumes were extremely high in light of the wireline network failure.

communications effort can serve as an important resource in future search and rescue endeavors. Separately, AT&T Wireless provided more than 5,000 wireless phones and free airtime to approximately 50 government agencies and organizations, including the Federal Emergency Management Agency, the Department of Transportation, the City of New York, and the Red Cross.

In the end, AT&T Wireless kept its network up and running, addressed urgent requests for service and equipment from displaced residential and business customers, emergency response agencies, and utility workers, and participated in coordinated search and recovery efforts. September 11 confirmed the critical importance of preparedness and collaboration in the face of disaster or terrorist attack. Looking ahead, AT&T Wireless firmly believes that the sharing of critical infrastructure information can provide the building blocks to identify and analyze vulnerabilities, develop plans to avert or reduce the impact of any attack, and establish restoration plans in the event of another attack or disaster. Achieving these goals will bring great benefits to both government and industry and will make all of us safer. AT&T Wireless is committed to helping advance these objectives.

III. INFORMATION SHARING AND IMPLEMENTATION OF THE CII ACT.

In February 2003, President Bush issued a report, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which sets forth “a foundation for building and fostering a cooperative environment in which government, industry, and private citizens can work together to protect our critical infrastructures and key assets.”⁴ It noted that the

⁴ Letter from the President introducing *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003), available at <http://www.whitehouse.gov/pcipb/physical.html> (“National Strategy Report”).

telecommunications sector's protection initiatives "are particularly important" because government and critical infrastructure industries rely so heavily on the public telecommunications infrastructure for vital communications.⁵ Indeed, as the experience of September 11 made so apparent, robust communications links – and, in particular, mobile wireless operations – are crucial to national security, to public safety, and to a connected citizenry. The *National Strategy Report* continued, noting:

Given the reality of the physical and cyber threats to the telecommunications sector, government and industry must continue to work together to understand vulnerabilities, develop countermeasures, establish policies and procedures, and raise awareness necessary to mitigate risks.⁶

To that end, AT&T Wireless supports the CII Act and the *Notice* to facilitate voluntary information sharing among industry participants and government. Assurance that industry submissions will be appropriately protected will facilitate such action. With regard to specific aspects of the *Notice*, AT&T Wireless urges DHS to clarify the proposed rules in three specific areas: the definition of critical infrastructure information; the presumption of protection; and intergovernmental coordination.

Critical Infrastructure Information Defined. Consistent with the provisions of the Homeland Security Act, the *Notice* defines critical infrastructure to mean physical or virtual systems and assets "so vital to the United States" that their incapacity or destruction "would have a debilitating impact on security, national economic security, national public health or safety, or

⁵ *National Strategy Report* at 48.

⁶ *Id.* at 49.

any combination thereof.”⁷ Every day, government agencies, critical industries, and ordinary citizens rely heavily on wireless communications services. As September 11 demonstrated, having wireless services available is crucial during a disaster event and in its immediate aftermath. These services clearly fall within the definition of critical infrastructure pursuant to the CII Act and the *Notice*.

Further, consistent with the CII Act, the *Notice* proposes to define critical infrastructure information to encompass information “not customarily in the public domain and related to the security of critical infrastructure or protected systems.”⁸ The *Notice* goes on to describe certain attributes of CII – information that concerns actual, potential or threatened interference or attack on critical infrastructure; the ability of critical infrastructure or protected systems to resist such interference or attack and any assessment of vulnerability, including risk management or risk audit information; or any planned or past recovery or reconstruction plans or solutions.⁹

While these descriptions of critical infrastructure information are useful, they are not sufficiently detailed. DHS should clarify that records or information that identify the location of critical infrastructure facilities or network elements, or that provide critical infrastructure network topology, are to be protected as critical infrastructure information. Network topologies, for example, would be important building blocks in a risk audit used to assess

⁷ *Notice*, 68 Fed. Reg. at 18525 (proposing 6 C.F.R. § 29.2(a)); *see also* 6 U.S.C. § 101(4) (citing 42 U.S.C. § 5195c(e)).

⁸ *Notice*, 68 Fed. Reg. at 18525 (proposing 6 C.F.R. § 29.2(b)); *see also* 6 U.S.C. § 131(3).

⁹ *See Notice*, 68 Fed. Reg. at 18525 (proposing 6 C.F.R. § 29.2(b)(1)-(3)); *see also* 6 U.S.C. § 131(3)(A)-(C).

telecommunications sector vulnerability (whether intra-sector or cross-sector).¹⁰ Such information, moreover, logically falls within the *Notice*'s proposed definition of protected CII, which includes records voluntarily submitted for use by DHS for "analysis" or "other informational purpose."¹¹ The threat of access to this information, however, poses a serious security risk and could deter the voluntary submission of such data. As a result, if DHS believes that network location information would be useful to its charge, it should make clear that such information will be treated as CII.

Presumption of Protection. AT&T Wireless strongly supports DHS's proposal that "[a]ll information submitted in accordance with the procedures set forth herein will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS."¹² Absent a presumption of protected status, there is very little likelihood that entities will choose to submit critical infrastructure information that poses a security risk. Simply put, a presumption of protection is necessary to effectuate the purpose of the CII Act.

Moreover, DHS should operate with the presumption of protection during the interim period prior to adoption of final rules. Congress directed DHS to ensure "uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information" within 90 days of enactment.¹³ In keeping with this directive, DHS should implement the presumption as

¹⁰ See *Notice*, 68 Fed. Reg. at 18525 (identifying "risk audit" as one example of critical infrastructure information in proposed 6 C.F.R. § 29.2(b)(2)).

¹¹ *Notice*, 68 Fed. Reg. at 18525 (proposing 6 C.F.R. § 29.2(f)).

¹² *Notice*, 68 Fed. Reg. at 18527 (proposing 6 C.F.R. § 29.6(b)).

¹³ CII Act, Section 214(e) (codified at 6 U.S.C. § 133(e)).

part of interim procedures, consistent with the policies underlying the CII Act, pending adoption of final rules.

Intergovernmental Coordination. In enacting the CII Act, Congress noted that nothing in the Act should be construed to limit the ability of a state, local, or federal agency from obtaining critical infrastructure information under other applicable law.¹⁴ Nonetheless, AT&T Wireless urges DHS to work with its colleagues at all levels of government to operate within a uniform framework for the collection and treatment of critical infrastructure information, consistent with the protections set forth in the CII Act. Public officials across the country are concerned – and rightly so – about the new threat environment and eager to take steps to reduce the likelihood of a terrorist act. With regard to critical infrastructure information, AT&T Wireless believes that a DHS-led framework with appropriate protections against unauthorized or unnecessary disclosure would better serve the public interest, in contrast to *ad hoc* information requests from jurisdictions throughout the country. AT&T Wireless thus suggests that DHS encourage its intergovernmental colleagues to work within the CII Act process in seeking critical infrastructure information.¹⁵

¹⁴ CII Act, Section 214(c) (codified at 6 U.S.C. § 133(c)).

¹⁵ See CII Act, Section 214(a)(1) (codified at 6 U.S.C. § 133(a)(1)).

IV. CONCLUSION

AT&T Wireless looks forward to working with DHS on critical infrastructure information issues and other issues that are so important to our nation's security, and supports DHS's adoption of rules consistent with the suggestions discussed above.

Respectfully submitted,

AT&T Wireless Services, Inc.

/s/

Douglas I. Brandon
Vice President – External Affairs
David Jatlow
Vice President – Federal Regulatory Affairs
1150 Connecticut Avenue, N.W.
Fourth Floor
Washington, D.C. 20036
(202) 223-9222