

5-2005


Homeland Security and Wireless Telecommunications: The Continuing Evolution of Regulation

Christopher Guttman-McCabe
CTIA-The Wireless Association

Amy Mushahwar
Catholic University

Patrick Murck
Catholic University

Follow this and additional works at: <http://www.repository.law.indiana.edu/fclj>

 Part of the [Administrative Law Commons](#), [Communications Law Commons](#), [Consumer Protection Law Commons](#), [Legislation Commons](#), and the [National Security Law Commons](#)

Recommended Citation

Guttman-McCabe, Christopher; Mushahwar, Amy; and Murck, Patrick (2005) "Homeland Security and Wireless Telecommunications: The Continuing Evolution of Regulation," *Federal Communications Law Journal*: Vol. 57: Iss. 3, Article 4. Available at: <http://www.repository.law.indiana.edu/fclj/vol57/iss3/4>

This Article is brought to you for free and open access by the Law School Journals at Digital Repository @ Maurer Law. It has been accepted for inclusion in Federal Communications Law Journal by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact wattn@indiana.edu.



JEROME HALL LAW LIBRARY

INDIANA UNIVERSITY
Maurer School of Law
Bloomington

HOMELAND SECURITY AND WIRELESS TELECOMMUNICATIONS: The Continuing Evolution of Regulation

Christopher Guttman-McCabe*

Amy Mushahwar**

Patrick Murck***

I. INTRODUCTION	415
II. PUBLIC INTEREST REGULATION IN THE NAME OF SAFETY.....	417
A. <i>Introduction</i>	417
B. <i>CALEA</i>	418
1. <i>CALEA Statutory Framework</i>	419
2. <i>Implementation on the Wireless Platform—Partnering Toward a Mandate</i>	421
a. <i>CALEA, an Industry Standard Initiative?</i>	422

* Christopher Guttman-McCabe is an Assistant Vice President, Regulatory Policy and Homeland Security at CTIA—The Wireless Association™. The views expressed in this article represent the views of the authors and do not necessarily reflect the views of CTIA or any of its member companies.

** Amy Mushahwar is a third year law student at Catholic University’s The Columbus School of Law and an Institute for Communications Law Studies certificate candidate.

*** Patrick Murck is a third year law student at Catholic University’s The Columbus School of Law and an Institute for Communications Law Studies certificate candidate.

<i>b. Law Enforcement Seeks to Revise the Industry Standard</i>	423
<i>c. The "Partnership" Moves to the Courtroom</i>	427
3. Packet-Based Implementation, Location Information, and Cost Concerns Add to the Uncertainty	427
<i>a. Compliance Issues</i>	429
<i>b. Deadline Extensions</i>	429
<i>c. Enforcement Regime</i>	430
<i>d. Cost Recovery</i>	430
C. <i>The E-911: To Partner or to Regulate?</i>	432
1. Introduction.....	432
2. Delivering E-911 Service in a Wireless Environment ...	434
<i>a. Background</i>	434
<i>b. Location Identification Alternatives</i>	435
3. Regulating a Consensus.....	436
<i>a. The Role of the Consensus Agreement in Shaping E-911 Regulation</i>	436
<i>b. The Cost-Recovery Problem</i>	437
III. THE EVOLUTION FROM PUBLIC SAFETY REGULATION TO HOMELAND SECURITY REGULATION.....	439
A. <i>Introduction</i>	439
B. <i>NRIC: The Foundation for Public-Private Partnerships</i>	440
1. NRIC's Historical Role in the Regulatory Process.....	440
<i>a. Preparing for Year 2000</i>	441
<i>b. Securing the Reliability of Telecommunications Networks</i>	441
2. NRIC's Newest Focus—Wireless	442
C. <i>Critical Infrastructure Information Act—Building the Foundation for Partnership</i>	443
1. Creation of the Act.....	443
2. Facilitating Information Sharing	444
D. <i>Reporting Wireless Network Outages</i>	445
E. <i>Wireless Priority Service: The Prototype of the Partnership Model</i>	447
1. The Call for Wireless Priority Service.....	448
2. Partnering for Success—Waivers, Liability Protection, and Funding	449
3. Deployment.....	451
4. Exporting the Partnership Model	452

<i>F. The Legacy of the Second Phase of Homeland Security Regulations</i>	452
IV. PHASE III: IN THE NAME OF HOMELAND SECURITY—TO PARTNER OR NOT?	453
V. CONCLUSION	454

I. INTRODUCTION

Since the grant of the first Commercial Mobile Radio Service (“CMRS”) license over twenty years ago, the wireless industry has grown from a service of convenience to one that is indispensable. What once was a device used for sporadic phone calls now is viewed by many Americans as a source of invaluable communication and security. Across the country, people use their wireless phones to make many, if not most, of their phone calls; some even have replaced their traditional land-line phones with wireless. Other people send emails or text messages, schedule appointments, browse the Internet, take pictures, listen to music, and even shop with their wireless phones. During the last twelve years, the number of wireless subscribers in the United States has grown from approximately 15 million to over 180 million,¹ while the annual minutes of use during the same time period have skyrocketed from below 20 billion to more than 1 trillion.² This rapid expansion has not been lost on government officials.

As the wireless industry has matured, government officials have turned to the mobile phone as a way to make the United States safer. E-911,³ the Communications Assistance for Law Enforcement Act (“CALEA”),⁴ Wireless Priority Service (“WPS”)⁵ and Outage Reporting⁶

1. See Cellular Telecommunications & Internet Association, Semi-Annual Wireless Industry Survey Results at <http://www.ctia.org/content/index.cfm/AID/10030> (last visited Apr. 2, 2005).

2. *Id.*

3. Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (1999) (codified at 47 U.S.C. § 251 (e)(3)). See also Enhance E-911 Act of 2004, Pub. L. No. 108-494, 2004 HR 5410 at § 102(4).

4. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at scattered sections of 18 U.S.C. and 47 U.S.C. §§ 1001-20).

5. The Development of Operation, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, Establishment of Rules and Requirements for Priority Access Service, *First Report and Order and Third Notice of Proposed Rulemaking*, 14 F.C.C.R. 152 (1998).

6. See New Part 4 of the Commission’s Rules Concerning Disruptions to Communications, *Report and Order and Further Notice of Proposed Rulemaking*, 19 F.C.C.R. 16,830 (2004).

all were initiated on the wireless platform in the name of safety. The Federal Communication Commission's ("FCC") implementation proceedings for these initiatives have differed markedly. Arguably, the differing FCC approaches significantly contributed to each initiative's outcome. Where the FCC fully partnered with industry, as in WPS, the service was operational in less than one year after being requested by government officials. Where government moved toward a more command and control approach, with multiple revisions to the rules, such as in E-911 and CALEA, the services still are not fully implemented. While blame can be spread across government and industry for the delays with E-911 and CALEA, an implementation model derived from the successful WPS approach bears review going forward. In an advanced technology area such as wireless, government goals may best be achieved by relying on industry experts as the technology is so sophisticated and constantly developing that the legislative and regulatory process at times cannot keep pace.

This Article will review wireless Public Safety and Homeland Security initiatives in three distinct phases. The first, involving CALEA and E-911, represents a phase whereby the FCC would *take into consideration* industry concerns and opinions as it moved toward the ultimate goal of regulation. The second phase, involving WPS and Outage Reporting, and occurring simultaneously with adoption of the Critical Infrastructure Information Act ("CIIA"),⁷ represents a regulatory and legislative movement to actually *replace certain potential regulations* with industry-initiated efforts and private-public partnerships. While not a full rejection of the first phase "regulatory mandate" approach, since Outage Reporting ultimately was mandated, this phase clearly represents a move by the FCC away from simple regulation and toward industry-government partnerships. Congress recognized this movement and adopted the CIIA to facilitate the sharing of information between industry and government.

The third phase currently is underway and involves issues such as emergency alert services⁸ and protection of critical infrastructure.⁹ As more Americans carry wireless phones and wireless minutes of use continue to grow dramatically, and as wireless handset capabilities and networks continue to expand, the government's focus on wireless service is a

7. See Critical Infrastructure Information Act of 2002, Pub.L. No. 107-296 (2002) (codified at 6 U.S.C. §§131-134).

8. *ee* Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, *Notice of Proposed Rulemaking*, 19 F.C.C.R. 4995 (2004).

9. The telecommunications industry, including the wireless industry, is considered one of the Nation's critical infrastructures. DEPARTMENT OF HOMELAND SECURITY, National Response Plan (2005) available at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml.

certainty. The key question is what type of regulatory approach the government will choose for this third phase.

E-911 and CALEA were an attempt by the FCC to regulate the telecommunication industry regarding very technical issues under difficult circumstances. The results have been far from perfect. WPS, also involving a very technical issue, was quickly and successfully implemented. Going forward, the industry obviously would like to convince the government that the best path toward achieving the government's wireless goals is to replicate the WPS model whenever possible.

This Article will explore the evolution of Homeland Security regulation of the wireless industry. Section II will detail early regulation of the industry initiated in the name of public interest and safety. Additionally, Section II will provide a detailed overview of both E-911 and CALEA and will discuss government actions that arguably delayed deployment of these initiatives. Section III will explore the evolution from public interest regulation to Homeland Security regulation after September 11, 2001 ("9/11"). One key element of this evolution is government's call for private-public partnerships. In this phase we see regulators move from direct regulation of licensees, to a more market-oriented, partnership approach. Section III will address Priority Access Services, the FCC's efforts to monitor service disruptions and report outages to wireless networks; the Network Reliability and Interoperability Council ("NRIC"); and the CIIA. Section IV will investigate emerging wireless industry Homeland Security issues, including Emergency Alert Services and the protection of critical infrastructure. Section IV will also discuss the regulatory approach that the government should employ. Section V will conclude that during this time of great uncertainty—in terms of both the evolution of the wireless industry and the safety and protection of our country—the trend to partner with the industry to reach government's goals is sensible and will benefit the American public.

II. PUBLIC INTEREST REGULATION IN THE NAME OF SAFETY

A. *Introduction*

The wireless issues surrounding CALEA, E-911 services, Priority Access, and Outage Reporting all emerged from the traditional wireline environment. The migration to parallel "public interest and homeland security" requirements and functionalities on the wireless network began with CALEA and E-911. While establishment of both of these regulations on the wireless platform involved significant input from industry, provision of CALEA and E-911 never was intended to be voluntary. This Section

traces the history of these early regulations from their wireline origins to the wireless mandate; addresses the elements of the proceedings, including the multiple FCC proceedings that arguably have led to uncertainty,¹⁰ that may have contributing to over a decade-long development cycle for both initiatives. This Section argues that the delay in full deployment of these services is linked, at least in part, to the regulatory approach that the FCC chose and the regulatory uncertainty that followed.

B. CALEA

Enacted in 1994, CALEA¹¹ codifies the government's ability to obtain government access to communications systems.¹² Congress wrote CALEA to extend and clarify the previous obligations of telecommunications service providers to assist law enforcement with electronic surveillance orders.¹³ CALEA not only preserved the government's existing rights to

10. "Federal and state regulators must remain cognizant that for industries with large investments in long-lived assets and long cycles for product and service development, regulatory uncertainty or churn has substantial costs." Leonard J. Kennedy & Heather A. Purcell, *Wandering Along The Road To Competition And Convergence—The Changing CMRS Roadmap*, 56 Fed. Comm. L.J. 489, 550 (2004) (citing Warren G. Lavey, *Making and Keeping Regulatory Promises*, 55 Fed. Comm. L.J. 1, 10 (2002)).

11. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in various sections of 18 U.S.C. and 47 U.S.C. §§ 1001-20).

12. H.R. REP. NO. 103-827 at 3489-90. This states that the purpose of CALEA as: [t]o insure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability to: (1) isolate expeditiously the content of targeted communications transmitted by the carrier within the carrier's service area; (2) isolate expeditiously information identifying the origin and destination of targeted communications; (3) provide intercepted communications and call identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and (4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications. The bill allows industry to develop standards to implement these requirements. It establishes a process for the Attorney General to identify capacity requirements.

Id.

13. In addition to the constitutional Fourth Amendment search and seizure limitations on government surveillance such as *Katz v. United States*, telecommunications providers have been subject to electronic surveillance legislation since 1968. 389 U.S. 347, 360 (1967) (Harlan, J., concurrence). Previous legislation includes the Omnibus Crime Control and Safe Streets Act, the Foreign Intelligence Surveillance Act, and the Electronic Communications Privacy Act. The Omnibus Crime Control and Safe Streets Act, ("OCCSSA") began as a check on law enforcement; it stated the procedure by which law enforcement could obtain an electronic surveillance order. Pub. L. No. 90-351, 82 Stat. 212 (1968). However, later amendments to the OCCSSA required telecommunication carriers to provide access points

circuit-switched telecommunications intercept, it also extended law enforcement's intercept rights to digital and wireless telephony.¹⁴ What Congress could not have anticipated was that CALEA, would lead to years of uncertainty and countless FCC and legal proceedings.

1. CALEA Statutory Framework

Section 103 of CALEA requires telecommunications providers¹⁵ to ensure that their equipment, facilities, and services adhere to standards that enable law enforcement to pursue call intercepts,¹⁶ pen registers,¹⁷ and trap and trace technologies¹⁸ for surveillance.¹⁹ The carrier cost for compliance

for intercept.

The Foreign Intelligence Surveillance Act ("FISA") authorized federal agencies to conduct electronic surveillance on a foreign power or agent and extended the budding obligations of telecommunication service providers. 50 U.S.C. §§ 1801–62. FISA requires all common carriers to furnish "all information, facilities or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference. . . ." 50 U.S.C. § 1801.

The Electronic Communications Privacy Act, broadened OCCSSA to include email, data transmissions, faxes, and pagers. Pub. L. No. 99-506 (1986).

14. See Hildegarde A. Senseney, *Interpreting the Communications Assistance for Law Enforcement Act of 1994: The Justice Department versus the Telecommunications Industry and Privacy Rights Advocates*, 20 HASTINGS COMM. & ENT. L.J. 665, (1998).

15. CALEA applies to "telecommunications carriers," the term under the statute includes any "person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." 47 U.S.C. §1001(8) (2000).

16. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, CALEA IMPLEMENTATION UNIT, FLEXIBLE DEPLOYMENT ASSISTANCE GUIDE: FURTHER EXTENSIONS OF THE JUNE 30, 2004 CALEA ASSISTANCE CAPABILITY REQUIREMENTS AND COMPLIANCE DATES, 4TH ED., May 2004, at 2, available at <http://www.askcalea.net/docs/flexguide4.pdf> [hereinafter DEPLOYMENT ASSISTANCE GUIDE] ("The term interception . . . refers to the lawful acquisition of the contents of any wire, electronic or oral communication . . . transmitted from one party to another.").

17. DEPLOYMENT ASSISTANCE GUIDE, *supra* note 16, at 3 ("The term pen register . . . refers to the lawful acquisition of certain outgoing dialing, routing, addressing or signaling information."). See also *Smith v. Maryland*, 442 U.S. 735, 736 n.1 (1979)

A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed. A pen register is usually installed at a central telephone facility and records on a paper tape all numbers dialed from the line to which it is attached.

Id. (internal citations omitted). While the *Smith* case explains older technologies used in pen register devices, the concept is the same. A pen register records outbound information dialed by the customer and does not record or transmit the contents of a telephone conversation. *Id.*

18. DEPLOYMENT ASSISTANCE GUIDE, *supra* note 16, at 3 ("[T]rap and trace . . . refers to the lawful acquisition of dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.").

19. CALEA at §103(a) (excerpted below).

(a) CAPABILITY REQUIREMENTS- Except as provided in subsections (b), (c),

with section 103 was capped at \$500 million for pre-1995 upgrades; telecommunications carriers were allocated reimbursement funding to meet those costs.²⁰ Carriers initially were required to be in compliance with CALEA by October 25, 1998.²¹

In addition to mandating access for electronic surveillance, section 103(a)(4) requires that common carriers preserve the privacy of their customers. Specifically, it commands that common carriers should not disclose "call-identifying information" that is "not authorized to be intercepted."²² Generally, in the mobile environment, if access to call-identifying information has not been authorized under a subpoena to the carrier, no information regarding the physical location of the mobile caller can be provided.²³

and (d) of this section and sections 108(a) and 109(b) and (d), a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier—[Sections 2 (A)–(B) omitted]

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information.

20. Center for Democracy and Technology, Status Report on the Communications Assistance for Law Enforcement Act: FBI Seeks to Impose Surveillance Mandates on Telephone system; Balanced Objectives of 1994 Law Frustrated, Mar. 4, 1999, available at http://www.cdt.org/digi_tele/status.htm [hereinafter Status Report on CALEA].

21. CALEA at §111(b).

22. See CALEA at §103(a)(4)(A); §103(a)(4)(B).

23. Jared J. Nylund, *Fire with Fire: How the FBI Set Technical Standards for the Telecommunications Industry Under CALEA*, 8 Comm. L. Conspectus 329, 334 (2000).

2. Implementation on the Wireless Platform—Partnering Toward a Mandate

As part of CALEA, Congress delegated to industry organizations the determination of the initial standards for compliance.²⁴ The effort to work with industry on a standard that ultimately would be imbedded in a mandate highlights the key element of the first phase of public safety regulation—working with industry toward the goal of regulation. Section 107 of CALEA contains a safe harbor provision that permits carriers to comply with CALEA simply by following the applicable industry standard.²⁵ Because of this safe harbor, CALEA appears to be an effort towards a government-industry partnership.

Two important components of CALEA, however, illustrate that it is part of this first phase of public interest and public safety regulation and demonstrate that the Act was not designed to be a truly voluntary industry initiative. First, the absence of a standard created by industry does not exempt telecommunications carriers from complying with the CALEA statute.²⁶ With or without a standard, CALEA compliance is mandatory, not voluntary. Second, the industry safe harbor is subject to FCC review under section 107(b) of CALEA.²⁷

24. See CALEA §107(a), 47 U.S.C. § 1006(a) (Supp. 2002).

25. *Id.* § 1006(a)(2). The section states:

COMPLIANCE UNDER ACCEPTED STANDARDS- A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103.

26. *Id.* § 1006(a)(3).

27. *Id.* § 1006. This section specifically states:

(b) **COMMISSION AUTHORITY-** If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that—

- (1) meet the assistance capability requirements of section 103 by cost-effective methods;
- (2) protect the privacy and security of communications not authorized to be intercepted;
- (3) minimize the cost of such compliance on residential ratepayers;
- (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of

Section 107(b) delegates to the FCC the power to regulate CALEA compliance if the industry fails to set a standard *or* upon petition to the FCC should the industry standard be found insufficient.²⁸ Congress empowered the FCC to supplant or amend the industry standard to accomplish the following goals: to meet the compliance requirements of section 103; to protect the privacy and security of communications; to minimize cost of compliance to residential ratepayers; to promote new technologies and services to the public; and to provide a deadline and compliance conditions during the CALEA transition period.²⁹ Together, the fact that the absence of a standard created by industry does not exempt telecommunications carriers from compliance combined with the ability of the FCC to review the industry safe harbor clearly reserve control over industry compliance to the FCC.

a. CALEA, an Industry Standard Initiative?

Shortly after the adoption of CALEA, Telecommunications Industry Association (“TIA”)³⁰ and Alliance for Telecommunications Industry Solutions (“ATIS”)³¹ established the first CALEA standard.³² Published in 1997, the first version of the standard J-STD-025 (“J Standard”)³³ was to serve as the safe harbor for wireline and wireless providers, as well as equipment manufacturers, under section 107(a)(2) of CALEA.³⁴ Despite

telecommunications carriers under section 103 during any transition period.

Id.

28. *Id.*

29. *Id.*

30. Telecommunications Industry Association, Communications Assistance for Law Enforcement Act, at <http://www.tiaonline.org/policy/calea/index.cfm> and <http://www.tiaonline.org/about/overview> (last visited Apr. 2, 2005) [hereinafter TIA] (stating that TIA is a trade association which represents “providers of communications and information technology products and services for the global marketplace through its core competencies in global standards development domestic and international advocacy, as well as market development and trade promotion programs.”).

31. Alliance for Telecommunications Industry Solutions Website, available at <http://www.atis.org/about.shtml> (stating that the Alliance for Telecommunications Industry Solutions (ATIS) is a standard setting body, and more than 350 communications companies participate in the body’s 22 industry committees.).

32. TIA, *supra* note 30 (stating that in early 1995, TIA began the standard setting process for CALEA compliance through its Engineering Subcommittee TR-45.2).

33. Press Release, Telecommunications Industry Association, TIA and ATIS Publish Lawfully Authorized Electronic Surveillance Industry Standard (Dec. 5, 1997) at http://www.tiaonline.org/pubs/press_releases/1997/97-96.cfm.

34. Communications Assistance for Law Enforcement Act and Broadband Access and Services, *Notice of Proposed Rulemaking and Declaratory Ruling*, 19 F.C.C.R. 15,676, paras. 12-13 (2004) [hereinafter *CALEA 2004 NPRM*]

the joint industry effort, the FBI strongly objected, which became the basis for a lengthy ongoing regulatory and legal battle. From this point forward, the industry no longer had full control of the standard-setting process, as the FCC entered the process under the role reserved to it in section 107(b) of CALEA.

b. Law Enforcement Seeks to Revise the Industry Standard

Although TIA and ATIS rewrote the standard to comply with the FBI's requirements in many respects, the FBI was not fully satisfied.³⁵ As a result, while the J Standard ultimately was adopted, it was merely an interim standard.³⁶ The FBI, along with thirty-five law enforcement agencies, soon shared their concerns regarding the J Standard with the FCC.³⁷ The FBI's multiple objections to the standard and the FCC's efforts to address those concerns began a cycle of law enforcement objections and FCC proceedings that arguably significantly impacted the timing of full CALEA implementation.

The first series of FBI objections concerned the extension of the October 1998 compliance deadlines. In a series of comments, the FBI objected to the requests of carriers, such as AT&T Wireless,³⁸ Bell South Cellular,³⁹ and US West, Inc.,⁴⁰ to extend the October 1998 CALEA compliance deadlines.⁴¹ The FBI argued that CALEA does not permit

35. Status Report on CALEA, *supra* note 20.

36. *Id.*

37. See Communications Assistance for Law Enforcement Act, *Comments of the Federal Bureau of Investigation Regarding Implementation of the Communications Assistance for Law Enforcement Act*, CC Dkt. No. 97-213 (1997). This first comment was submitted one month after the J Standard was published. It merely stated that the current standards process was ongoing and it was inappropriate to specifically comment on the standard at that time. *Id.* See also Communications Assistance for Law Enforcement Act, *Reply Comments of the Federal Bureau of Investigation Regarding Implementation of the Communications Assistance for Law Enforcement Act*, CC Dkt. No. 97-213 (1998), available at <http://www.askcalea.net/docs/980211.pdf> [hereinafter *1998 FBI Reply Comments*].

38. See, e.g., Communications Assistance for Law Enforcement Act, *Comments of AT&T Wireless*, CC Docket No. 97-213 (1998).

39. Communications Assistance for Law Enforcement Act, *Comments of Bell South Cellular*, CC Docket No. 97-213 (1998).

40. See, e.g., Communications Assistance for Law Enforcement Act, *Comments of U.S. West, Inc.*, CC Dkt. No. 97-213 (1998). See also, *1998 FBI Reply Comments*, available at <http://www.askcalea.net/docs/980211.pdf> (providing that the FBI was particularly opposed to U.S. West's reading of the statute. U.S. West argued that section 107(c), the extension provision of the statute, "does not limit the Commission's authority to granting extensions based on individual carrier petitions.").

41. Carriers were asking for a two-year extension to October 24, 2000. They pointed to many reasons for the necessity of a compliance extension, including equipment difficulties,

industry-wide deadline extensions.⁴² Even with the FBI's objections, the FCC eventually extended CALEA compliance until June 30, 2000.⁴³ This extension did not come without controversy. In addition to opposing the extensions, the FBI also requested a series of CALEA standard capabilities not incorporated in TIA's J Standard.⁴⁴ Thus, the voluntarily developed industry-driven standard was going to be revised by the government.

A little more than a month after the FBI filed Reply Comments in 1998, it issued its "Punch List" of specific technical requirements to be included in the J Standard. These requirements were listed in a Joint Petition for Expedited Rulemaking filed by the FBI and the Department of Justice,⁴⁵ under section 107 (b) of the CALEA, which allows that "if a

and roving standards, to name a few. *See e.g.*, Petition for Extension of the Compliance Date under section 107 of the Communications Assistance for Law Enforcement Act, ICG Telecom Group, Inc. Petition for Extension and Comments, CC Docket No. 97-213 (1998) (providing that ICG cited difficulties in obtaining CALEA compliant equipment as the thrust of its extension petition. In fact, ICG's primary vendor, Lucent Technologies, Inc., filed a CALEA extension petition as well. ICG argued that it couldn't possibly be compliant if its vendor was doubtful of compliance); Petition for an Extension of the CALEA Assistance Capability Compliance Date of the Communications Assistance for Law Enforcement Act, Air Touch Paging, Inc., Petition for an Extension of the CALEA Assistance Capability Compliance Date, CC Docket No. 97-213 (1998) (providing that AirTouch Paging originally thought its clone paging system was compliant with CALEA. However, it stated that the FBI in 1998 changed its position and stated that clone pagers were not compliant with the statute. AirTouch states that the FBI found them in compliance as early as December 1997). In addition to these and many other named carriers, trade associations, such as CTIA, TIA, and the Personal Communications Industry Association also commented on the proceeding. The FBI would later comment that trade associations do not have administrative standing to participate in a time extension request. *1998 FBI Reply Comments, supra* note 37, paras. 7-8.

42. *See 1998 FBI Reply Comments, supra* note 37, paras. 7-13.

43. *See* Petition for the Extension of the Compliance Date Under Section 107 of the Communications Assistance for Law Enforcement Act by AT&T Wireless Services, Inc, *Memorandum Opinion and Order*, 13 Comm. Reg. (P & F) 432 (1998), available at <http://ftp.fcc.gov/Bureaus/Wireless/Orders/1998/fcc98223.pdf> [hereinafter *AT&T Petition Opinion and Order*]. After the 1998 extension, the Commission extended the compliance deadline twice. The most recent extension period expired on January 1, 2004; *see* notes for a discussion of the most recent NPRM (explaining that the current NPRM has tentatively concluded that blanket extensions will not be granted).

44. *1998 FBI Reply Comments, supra* note 37, paras. 55-91 (providing that CALEA compliance improvement items included extending civil liabilities to carriers whose employees unlawfully intercept communications, requiring carriers to designate specific personnel to CALEA matters, requiring adequate recordkeeping, assistance affidavits for carrier personnel, employee violation reporting procedures, timeliness requirements for intercept requests, and certification of CALEA requirement for all carriers).

45. Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities under the Communications Assistance for Law Enforcement Act, *Joint Petition for Expedited Rulemaking* (1998) available at <http://www.askcalea.net/docs/980327.pdf> [hereinafter *Punch List Petition*].

Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the FCC to establish, by rule, technical requirements or standards.⁴⁶ The Joint Petition sought the following requirements to cure the perceived J Standard deficiencies:

Access to the communications of all parties in a conference call supported by the subscriber's service or facilities; -Access to all subject-initiated dialing and signaling activity; -Information indicating whether a party is connected to a multi-party call at any given time ("party hold," "party join," and "party drop" messages); -Notification of messages for in-band and out-of-band signaling; -Timely delivery of call-identifying information; -Automated reporting of surveillance status; -Delivery of all call-identifying information over call data channels; and-A limited number of standardized delivery interfaces.⁴⁷

The Center for Democracy and Technology estimated that the FBI wish list would increase compliance costs from \$500 million to between \$3 and \$5 billion.⁴⁸ In addition to the proposed "punch list" changes, the FBI sought to shift the total cost of compliance to carriers.⁴⁹ These proposed changes and looming cost recovery issues added to the uncertainty surrounding CALEA.

The FCC's resultant third Report and Order held that six of the "punch list" items were within the scope of CALEA call-identifying information.⁵⁰ Specifically, packet mode communications capabilities⁵¹ and location information⁵² capabilities were required to be part of the J

46. See CALEA at §107(b) (codified at 47 U.S.C. § 1006 (b)).

47. *Punch List Petition*, *supra* note 45, para. 35.

48. STATUS REPORT ON CALEA, *supra* note 20.

49. *Id.* See also *Punch List Petition*, *supra* note 45, para. 112 (recognizing that the Commission had previously issued a rulemaking proceeding on the subject of cost recovery).

50. Communications Assistance for Law Enforcement Act, *Third Report and Order*, 14 F.C.C.R. 16,794, paras. 74, 82, 89, 95, 119 (1999) available at <http://www.askcalea.com/docs/fcc99230.pdf> (providing that the following capabilities were required to be included in the J Standard: party hold/join/drop information, subject-initiated dialing and signaling information, in-band and out-of-band signaling that constitutes call-identifying information, a timing information requirement, and digits dialed after connecting to a carrier also constitute call identifying information).

51. CALEA 2004 NPRM, *supra* note 34, para. 14 n.24 ("Section 3 of the J Standard describes packet-mode as a 'communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by accessing [a] telecommunication[s] system. Each packet may take a different route through the intervening network(s).").

52. *Id.* para. 14 n.25

The J Standard includes a parameter that identifies the location of a subject's "mobile terminal" whenever this information is reasonably available and its delivery to a LEA [law enforcement agency] is legally authorized. Location

Standard. This Order further illustrated the government's control over the CALEA standard process.

Carriers immediately were concerned that traditional dividing lines securing certain consumers' communications could not translate into packet-based communications under the new CALEA requirements.⁵³ If law enforcement intercepted packets from a wireless customer, those packets would contain both location information, in the header of the packet, as well as call content in the payload segments of the packet.⁵⁴ If law enforcement did not obtain a full call intercept warrant, the government could obtain greater information than it was legally authorized to access. Law enforcement in this instance could be engaging in an unlawful search contrary to the statute and legal precedent.⁵⁵ TIA noted that with packet-based technologies the "responsibility [is] on the [law enforcement agent] to retain only the authorized information. . . ."⁵⁶ Carriers eventually petitioned the D.C. Circuit for relief of the packet mode requirements, the location information capabilities, and four other "punch list"

information is available to the LEA irrespective of whether a call content channel or a call data channel is employed.

Id.

53. Betsy Harter, *CALEA Irks Carriers*, WIRELESS REVIEW, Oct. 1, 1999, available at http://wirelessreview.com/ar/wireless_calea_irks_carriers.

54. Joint Experts Meeting convened by Committee TR 45 of the Telecommunications Industry Association, Report to the Federal Communications Commission on Surveillance of Packet-Mode Technologies, (Sept. 29, 2000) available at http://www.tiaonline.org/government/filings/JEM_Rpt_Final_092900.pdf [hereinafter TIA Report]. The Report stated:

Currently J-STD-025 specifies delivery of the entire packet stream or just the Source and Destination address information for a user under surveillance. While delivery of the entire packet stream guarantees that authorized Pen Register and Trap and Trace information will be delivered to the LEA, it does not remove content prior to delivery.

55. Ordinarily, a LEA is required to obtain a warrant supported by probable cause prior to the grant of an intercept order. *Katz v. United States*, 389 U.S. 347 (1967) (overruling the trespass doctrine of *Olmstead v. United States* and holding that FBI agents conducted a Fourth Amendment search when they attached an electronic listening device to a telephone booth); *contra Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a pen register does not constitute a Fourth Amendment search, and as such a warrant is not required for the conduct). Note that the Electronic Communications Privacy Act of 1986 ("ECPA") does require law enforcement to obtain a certification for a pen register. However, this pen register order only requires a law enforcement officer to certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2)); see also 18 U.S.C. § 2511(2)(h) (stating that a pen register is not an unlawful intercept under Title III of the Omnibus Crime Control and Safe Streets Act of 1968). As such, an LEA could request a pen register which does not have a warrant requirement, and possibly receive call content.

56. TIA Report, *supra* note 54, at 15.

requirements.⁵⁷

c. The “Partnership” Moves to the Courtroom

What began as an industry-government partnership ultimately moved to the courtroom, as the uncertainty surrounding CALEA compliance grew. The United States Telecom Association (“USTA”) and other petitioners sued in the D.C. Circuit seeking a review of the Third Report and Order and a limitation on expansion of CALEA requirements.⁵⁸ In particular, the petitioners questioned the legality of the packet-mode capability requirement,⁵⁹ the location information requirement,⁶⁰ and four of the six “punch list” items.⁶¹ The court vacated the “four punch” list items in part; however, the FCC, in an Order on Remand, found that CALEA mandated all punch list capabilities.⁶² The Order on Remand was not appealed again by USTA or any other telecommunications provider or association.⁶³ As such, all six “punch list” items became part of the CALEA requirements. This regulatory action provided further evidence that the “safe harbor” review process was not part of a voluntary industry-government partnership; but rather part of a traditional industry mandate.

3. Packet-Based Implementation, Location Information, and Cost Concerns Add to the Uncertainty

Although in the intervening years some of the wireless industry’s concerns were addressed—including the creation by the FBI of a Flexible Deployment Program for compliance with the CALEA standards and

57. *CALEA 2004 NPRM*, *supra* note 34, para. 15 n.30 (providing that carriers challenged the following punch list requirements in addition to the location information and packet mode requirements: “dialed digit extraction, party hold/join/drop, subject initiated dialing and signaling, and in band and out-of-band signaling.”).

58. *United States Telecomm. Ass’n v. FCC (USTA)*, 227 F.3d 450, 450 (D.C. Cir. 2000).

59. *Id.* at 464 (providing that the packet mode capability requirement dealt with the inability to separate packet location information in its header from call content in the packet payload).

60. *Id.* (discussing that the location information provision required wireless carriers to make available the physical location of the nearest antenna tower at the beginning and end of each call. CDT stated that this requirement effectively “converts ordinary mobile telephones into personal location-tracking devices. . .”).

61. *Id.* at 456 (providing that petitioners challenged dialed digit extraction, party hold/join/drop, subject initiated dialing and signaling, and in-band and out-of-band signaling).

62. *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Order on Remand*, 17 F.C.C.R. 6896 (2002) [hereinafter *2002 Order on Remand*]. *See also*, *CALEA 2004 NPRM*, *supra* note 34, para. 15.

63. *CALEA 2004 NPRM*, *supra* note 34, para. 15

extended compliance deadlines pertaining to packet-mode petitions—much continues to remain uncertain regarding CALEA compliance.⁶⁴ This uncertainty is due both to the technical complexity of the issue as well as the multiple changes to the standard and the rules.⁶⁵ This uncertainty continues. Despite close to a decade of regulatory inquiry, a 2004 Joint Petition identified thirteen issues regarding CALEA.⁶⁶

The FCC responded with a Notice of Proposed Rulemaking and Declaratory Ruling (“CALEA 2004 NPRM”) that once again raised a host of new issues surrounding CALEA compliance.⁶⁷ In addition to addressing

64. DEPLOYMENT ASSISTANCE GUIDE, *supra* note 16 (explaining that the FCC established a deadline for packet-mode communications compliance which is January 30, 2004). See also Wireline Competition and Wireless Telecommunications Bureaus Announce a Revised Schedule for Consideration of Pending Packet Mode CALEA Section 107(c) Petitions and Related Issues, *Public Notice*, 18 F.C.C.R. 24,243 (2003)

65. United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, *Joint Petition for Expedited Rulemaking* (2004) available at <http://www.askcalea.net/docs/20040310.calea.jper.pdf> [hereinafter *2004 Joint Petition*].

66. *Id.* at iii. The Joint Petition asked the Commission to:

- (1) formally identify the types of services and entities that are subject to CALEA;
- (2) formally identify the services that are considered “packet-mode services”;
- (3) initially issue a Declaratory Ruling or other formal Commission statement, and ultimately adopt final rules, finding that broadband access services and broadband telephony services are subject to CALEA;
- (4) reaffirm, consistent with the Commission’s finding in the *CALEA Second Report and Order*, that push-to-talk “dispatch” service is subject to CALEA;
- (5) adopt rules that provide for the easy and rapid identification of future CALEA-covered services and entities;
- (6) establish benchmarks and deadlines for CALEA packet-mode compliance;
- (7) adopt rules that provide for the establishment of benchmarks and deadlines for CALEA compliance with future CALEA-covered technologies;
- (8) outline the criteria for extensions of any benchmarks and deadlines for compliance with future CALEA-covered technologies established by the Commission;
- (9) establish rules to permit it to request information regarding CALEA compliance generally;
- (10) establish procedures for enforcement action against entities that do not comply with their CALEA obligations;
- (11) confirm that carriers bear sole financial responsibility for CALEA implementation costs for post-January 1, 1995 communications equipment, facilities and services;
- (12) permit carriers to recover their CALEA implementation costs from their customers; and
- (13) clarify the cost methodology and financial responsibility associated with intercept provisioning.

Id.

67. *CALEA 2004 NPRM*, *supra* note 34.

push-to-talk services and packet mode technologies,⁶⁸ the FCC questioned threshold service definitions, CALEA extensions, and cost recovery.⁶⁹

Throughout the proceeding, as the FCC addressed certain issues, it often raised additional questions that continued the march toward a traditional mandate. For example, the threshold question of how to define for regulatory purposes whether certain carriers are “telecommunications carriers” under the statute and thus subject to the CALEA is now—eleven years after its enactment—being considered by the industry and the FCC. The CALEA 2004 NPRM tentatively concludes that facilities-based providers of broadband telephony are subject to CALEA’s requirements as is any non-facilities-based provider that constitutes a substantial replacement of wire services, including wireless carriers.⁷⁰

a. Compliance Issues

Many compliance questions also remain. First, the inclusion of location information or call identifying information in any data retrieved by government persists as a concern to carriers.⁷¹ The FCC previously determined that, per CALEA, call identifying information was not limited to telephone numbers; therefore, mobile service providers could include the physical locations of antenna towers used to connect the call.⁷² In the CALEA 2004 NPRM, the FCC realized that the location information for the packet may not be reasonably identifiable without examining the packet’s content.⁷³ The FCC also sought comment on what *call-identifying information* is considered reasonably available per section 103(a)(2) of the CALEA.⁷⁴ These questions add to the level of uncertainty surrounding compliance with the CALEA requirements, and if past experience is any indication of future action, additional regulatory or legal proceedings are likely to follow.

b. Deadline Extensions

In the Notice of Proposed Rulemaking, the FCC also considered the subject of CALEA deadline extensions. Perhaps due in part to the multiple

68. *Id.* at 3. (describing CALEA as being technology neutral).

69. 2002 *Order on Remand*, *supra* note 62.

70. *Id.* para. 37. Note, that CALEA Notice on Proposed Rule Making does explore non-facilities-based telephony providers, however this Article is limited to a discussion of issues facing the wireless carrier.

71. *Id.* paras. 63–68.

72. *Id.* para. 64.

73. *Id.* para. 65.

74. *Id.* paras. 66–67 (listing the three types of call-identifying information provided by the Act).

changes in the CALEA requirements, extensions continue to flow into the FCC. Over 750 CALEA extension petitions were filed prior to June 30, 2004.⁷⁵ The FCC voiced support for tightening extension deadlines and tentatively concluded that ninety days is a reasonable period of time to comply with CALEA's requirements.⁷⁶ The FCC also sought comment on whether the FBI program should function as a barometer of what is reasonably achievable under section 107(c) of the CALEA.⁷⁷

c. Enforcement Regime

Surprisingly, the CALEA 2004 NPRM also sought comment on additional threshold issues, including the appropriate enforcement regime for CALEA petitions.⁷⁸ The 2004 Joint Petition asked the FCC specifically to outline the enforcement actions that need to be taken against carriers and equipment manufacturers.⁷⁹ The FCC sought comment on whether it may take separate enforcement action against carriers and manufacturers that fail to comply with CALEA.⁸⁰

d. Cost Recovery

Finally, cost recovery issues have been raised by the FCC. The FCC recognized that CALEA required capital expenditures and continuing expenses by the wireless community.⁸¹ Law enforcement argued that the burden of CALEA cost should be placed on the carriers and not the local law enforcement agencies ("LEAs").⁸² The 2004 CALEA NPRM identified

75. *Id.* para. 90. (Since then, the Commission has received an additional 330 new § 107(c) extension petitions). The Commission also recognized that some carriers are actively negotiating with the FBI through its Flexible Deployment Program. Under the FBI's Flexible Deployment program, a carrier provides the agency with all of its information regarding the switches in its network and the carriers' most recent surveillance assistance activity. With this data, the FBI will attempt to negotiate a mutual deployment schedule with the carrier. See Communications Assistance for Law Enforcement Act, Ask CALEA Website, Flexible Deployment, available at <http://www.askcalea.net/flexd.html> (last visited May 18, 2005).

76. CALEA 2004 NPRM, *supra* note 34 at para. 91 (providing that the Commission also leaves open the possibility that individual carriers may be seeking relief from the CALEA requirements).

77. *Id.* para. 93.

78. *Id.* paras. 111–116. See also 47 U.S.C. § 1007 (stating the current civil suit remedy for CALEA enforcement).

79. 2004 Joint Petition, *supra* note 65, at 58.

80. See, e.g., CALEA 2004 NPRM, *supra* note 34, para. 113.

81. *Id.* para. 117.

82. 2004 Joint Petition, *supra* note 65, at 64. See also 2004 CALEA NPRM, *supra* note 34, para. 123 n.295.

that CALEA section 109 provides for three cost recovery mechanisms.⁸³ As for equipment modifications prior to 1995, the federal government bears the costs for those upgrades; where it does not bear the cost, those pre-1995 facilities are considered CALEA compliant until the equipment or facilities are modified.⁸⁴

The FCC tentatively concluded that carriers are responsible for equipment and facilities developed after January 1, 1995.⁸⁵ The FCC, however, sought comment on whether specific rules are necessary to determine the carrier's compliance cost.⁸⁶ In addition to questions regarding reimbursement for modification of facilities, there also are questions regarding intercept-related costs.⁸⁷ Generally, LEAs must compensate wireless providers for specific intercept-related costs.⁸⁸ Law enforcement argues the government is charged twice for CALEA compliance. The LEA argument states that by including intercept costs, carriers are able to recover costs for hardware and software for post January 1995 equipment.⁸⁹ Additionally, the LEAs argued in their petition that the intercept-related costs improperly shifted the CALEA cost burden to the government when the government already provided funds for pre-1995 upgrades.⁹⁰

In essence, the 2004 Joint Petition and the *CALEA 2004 NPRM* represent over a decade of shifting toward a traditional mandatory regulation and away from the initial government-industry partnership. This movement is illustrative of the first phase of public safety and Homeland Security regulation. The CALEA safe harbor J Standard was developed to allow industry to adapt a compliant solution. Uncertainty, however, has been the norm since the establishment of that original standard. Actions by the government, including the most recent conclusions regarding

83. 2004 CALEA NPRM, *supra* note 34, para. 125.

(1) the costs of developing the modifications for equipment deployed on or before January 1, 1995, (2) the costs of providing the capabilities for equipment deployed after January 1, 1995, but only where the Commission finds compliance is not "reasonably achievable" and (3) the costs of providing the "capabilities" required under section 104 of CALEA. . . .

Id. The NPRM identifies that the costs of providing the capabilities is not at issue. *Id.* The D.C. circuit addressed the third issue in *United States Telecomm. Ass'n v. FBI*, 276 F.3d 620 (D.C. Cir. 2002)).

84. 2004 CALEA NPRM, *supra* note 34, para. 125.

85. *Id.*

86. *Id.*

87. *Id.* paras. 132–35.

88. *Id.* para. 132.

89. *Id.*

90. *Id.*

extensions and cost recovery, will continue the uncertainty. This ten-year process is a strong example of the lack of an effective government-industry partnership. Unfortunately, in this first phase of public safety and Homeland Security regulation, CALEA is not the only example of an ineffective partnership that ultimately led to delay.

C. *E-911: To Partner or to Regulate?*

1. Introduction

Uncertainty, confusion, and changes in the FCC's rules are not exclusive to CALEA. Working with industry on elements of compliance with a government mandate also is not exclusive to CALEA. Each of these CALEA experiences arose in the E-911 proceeding. Accordingly, the result for E-911 development and deployment is not unlike the result in CALEA. Countless regulatory and legal proceedings combined with significant uncertainty, resulted in a proceeding that is over ten years old. The proceeding illustrates the difficulties regulators encounter in trying to address the uncertainty of implementing mandates that involve new communications technologies.⁹¹

The path that the E-911 proceeding has taken over the last decade obviously is not a model for future industry-government partnerships, even though the proceeding arose from a general industry consensus that E-911 wireless services were needed. Despite the industry origins, the FCC decided that ultimately it was going to mandate the E-911 requirement. The question that arose during the initial phase of the proceeding was to what extent regulatory intervention was necessary.⁹²

Consistent with this phase of public safety regulation, the FCC initially relied on the ability of industry and public safety groups to develop the E-911 rules and regulations. The FCC imposed E-911 rules based

91. Warren G. Lavey, *Making and Keeping Regulatory Promises*, 55 Fed. Comm. L.J. 1, 39-40 (2002). "While regulators control access charges and universal funding mechanisms, they do not control, and often have poor visibility into, technological developments for some new services for a group of licensed carriers also involving equipment suppliers, interconnected carriers, and other non-carrier entities that play roles in provisioning the services. Repeated rule changes and recent waivers in this proceeding point to the fine line between enforceable commitments and nonenforceable statements of intentions." *Id.*

92. See Amendment of the Commission's Rules to Establish New Personal Communications Services, *Second Report and Order*, 8 F.C.C.R. 7700, paras. 139-140 (1993) [hereinafter *Second Report and Order*]. See also Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Report and Order and Further Notice of Proposed Rulemaking*, 11 F.C.C.R. 18,676, paras. 21, 61 (1996) [hereinafter *First E-911 Report and Order*].

largely upon a framework developed by representatives of the wireless industry and public safety organizations in a Consensus Agreement.⁹³ The Consensus Agreement had a profound impact on shaping the regulation of E-911. As with CALEA, the FCC retained a significant regulatory role in the development and deployment of E-911.

To a large extent the FCC, in implementing rules for the development of E-911, addressed Commissioner Kathleen Abernathy's suggestion that when regulating in a rapidly changing technological environment, the FCC should be eager "to reach out to a broad array of groups to maximize the information available to decision makers."⁹⁴ As stated above, the regulation of wireless E-911 was initially shaped by early industry-government partnerships.⁹⁵ The FCC's rigidity in applying certain aspects of this agreement,⁹⁶ as well as multiple revisions to the rules—at times at the request of the wireless industry—has created uncertainty for the industry, arguably hampering deployment.⁹⁷ Further, the FCC's attempts to adopt strict timetables based on vendor representations and in the face of rapid technological change arguably also impacted deployment of E-911, instead

93. *First E-911 Report and Order* at paras. 21, 61.

94. Kathleen Q. Abernathy, *My View From the Doorstep of FCC Change*, 54 *FED. COMM. L.J.* 199, 218 (2002).

95. See e.g., *First E-911 Report and Order*, *supra* note 92. See also Revision of the Commission's Rules to Ensure Compatibility with E-911 Emergency Calling Systems, *Second Memorandum Opinion and Order*, 14 F.C.C.R. 20,850, para. 1 (1999) [hereinafter *Second E-911 Report and Order*] (The Commission adopted E-911 rules in accordance with an agreement between the wireless industry and State and local 911 officials.).

96. See *Second E-911 Report and Order*, *supra* note 95 (discussing the Commission's enforcement measures regarding the timetable for E-911 deployment.).

97. See discussion of the Commission's decision to eliminate the cost-recovery requirement as it pertains to wireless carriers *infra* Part II.C.3.c. See also Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Comments of Western Wireless Corporation and VoiceStream Wireless Corporation*, CC Dkt. No. 94-102, at 2 (1999), available at http://gulfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6009451135 ("The initial obstacle in providing E-911 service is the lack of cost recovery legislation signed into law in many states."); Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Comments of APCO in Response to Public Notice of August 16, 1999*, CC Dkt. No. 94-102, at 3 (1999), available at http://gulfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6009451133 ("In particular, the extremely slow pace of cost-recovery legislation has been the principal impediment to implementing the Commission's E9-1-1 rules."); Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems, *Comments of the Rural Telecommunications Group*, CC Dkt. No. 94-102, at 2 (1999), available at http://gulfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6009450625 ("The absence of federal guidelines regarding the scope of recoverable costs makes the task of establishing procedures for collecting fees and distributing proceeds even more difficult. To accelerate implementation...the Commission [should] adopt uniform federal guidelines to guide the states in adopting cost recovery mechanisms.").

of creating market certainty as the FCC had hoped.⁹⁸

2. Delivering E-911 Service in a Wireless Environment

a. Background

Basic 911 service routes emergency calls to Public Safety Answering Points ("PSAPs").⁹⁹ When a 911 call is placed by a wireline customer, the phone number is identified through Automatic Number Identification ("ANI") technology and that number is matched to a database listing the corresponding address.¹⁰⁰ The call is then routed by the Local Exchange Carrier ("LEC") to the nearest PSAP.¹⁰¹ This constitutes wireline ALI. E-911 requires delivery of two elements. The first element is ANI, the second is Automatic Location Identification ("ALI").¹⁰²

For the wireless industry, the process and rules for satisfying E-911 requirements differ from those of the wireline industry. The ANI requirements for wireless require the carrier to provide both the number of the wireless user and the location of the cell site or base station.¹⁰³ The ALI rules for wireless carriers require the carrier to provide the physical location of the caller by longitude and latitude.¹⁰⁴ ALI is important both for allowing PSAPs to identify to a certain degree the location of a caller,¹⁰⁵ and for making sure that local wireline carriers route calls to the nearest PSAPs with greater accuracy than can be attained by merely using ANI.¹⁰⁶

The minimum standard of accuracy for wireless ALI is dependant on the type of technology used by the carrier.¹⁰⁷ As the industry and the FCC have learned, developing E-911 service in a wireless environment produces

98. See *infra* Part II.C.2.b.

99. Revision of the Commissions Rules to Ensure Compatibility with Enhanced 911 Emergency Calling System, *Notice of Proposed Rulemaking*, 9 F.C.C.R. 6170, para. 5 (1994).

100. *Id.* para. 4.

101. *Id.*

102. *First E-911 Report and Order*, *supra* note 92, paras. 4-5.

103. 47 C.F.R. § 20.18(d)(1) (2002).

104. *Id.* §20.18(e).

105. Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Third Report and Order*, 14 F.C.C.R. 17,388, para. 2 (1999) [hereinafter *Third E-911 Report and Order*].

106. *Id.*

107. See, e.g., 47 C.F.R. § 20.18(h)(1)-(2).

[N]etwork-based ALI carriers must determine the caller's location within 300 meters 95 percent of the time and 100 meters 67 percent of the time. . . .

[H]andset-based ALI carriers must determine the caller's location within 150 meters 95 percent of the time and 50 meters 67 percent of the time.

Id.

distinct challenges from wireline E-911,¹⁰⁸ presented primarily in delivery of ALI functionality. The FCC, working initially with both industry and public safety groups, divided the deployment of E-911 services into two phases. Phase I consisted of the deployment of ANI functionality, while Phase II consisted of the deployment of ALI functionality.¹⁰⁹ While there were some troubles implementing Phase I of the E-911 mandate,¹¹⁰ most of the disputes and uncertainty has centered on the development and satisfaction of Phase II requirements.¹¹¹

b. Location Identification Alternatives

In its Rules, the FCC did not mandate a particular ALI location solution for delivery of Phase II. Under the original E-911 plan adopted by the FCC, the wireless carriers had to use network-based ALI to meet their Phase I requirements.¹¹² However, after a revision of the initial rules, wireless carriers were able to choose either a handset-based or network-based solution.¹¹³ Handset-based ALI would utilize GPS and similar location technologies,¹¹⁴ while network-based ALI would use triangulation of the mobile signal and similar technologies.¹¹⁵

Both solutions have benefits and concerns attached. In urban areas, for example, a network-based solution may make more sense to some wireless carriers as the concentration of cellular towers in those areas makes triangulation easier.¹¹⁶ For rural areas, triangulation utilizing cell sites could require massive investment in new infrastructure to accommodate triangulation technologies.¹¹⁷ There are similar benefits and problems with use of a handset-based solution. . These issues are just two of the many that have been raised in this proceeding, highlighting E-911,

108. *First E-911 Report and Order*, *supra* note 92, para. 7 (“[T]he nature of wireless technology and service presents significant obstacles to making E-911 effective for wireless calls.”).

109. Dale N. Hatfield, A REPORT ON TECHNICAL AND OPERATIONAL ISSUES IMPACTING THE PROVISION OF WIRELESS ENHANCED 911 SERVICES 10–11, *available at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=651329623 9 [hereinafter HATFIELD REPORT].

110. *Second E-911 Report and Order*, *supra* note 95, para. 16.

111. *See infra* Part II.3.

112. *Third E-911 Report and Order*, *supra* note 105, para. 2.

113. *See, e.g., id.* (revising the FCC Phase II requirements to allow competition between network-based and handset-based technologies and to make Phase II benchmarks for ALI more stringent based on the technological advances that had occurred between the issuing of the first E-911 order and the third E-911 order).

114. HATFIELD REPORT, *supra* note 109, at 10–11.

115. *Id.* at 10.

116. *Id.* at 12.

117. *Id.*

along with CALEA, as being part of the first phase of public safety regulation.

3. Regulating a Consensus

a. *The Role of the Consensus Agreement in Shaping E-911 Regulation*

As in the early stages of the CALEA proceeding, “the Commission imposed E-911 rules . . . based largely upon a framework developed by representatives of the wireless industry and public safety organizations in a Consensus Agreement.”¹¹⁸ From the industry’s perspective, the FCC’s effort to partner with wireless carriers in the development of regulations initially was beneficial. However, while the Consensus Agreement had a profound impact on shaping the regulation of E-911,¹¹⁹ the FCC, as it did with CALEA, obviously carved out a role for the regulator as the final arbiter of what elements would be binding and which parts would be modified or eliminated.¹²⁰

The FCC’s approach to E-911 could be described as an attempt at goals-based partnership toward regulation. That is, the regulator established goals and minimum standards, while not initially mandating any specific method or practice for achieving those goals and standards. This regulatory method was illustrated in the FCC’s decision to revise the Phase II requirements to allow for handset-based ALI technologies.¹²¹

The same approach held when establishing a deadline for compliance. The FCC followed the recommendations of the Consensus Agreement.¹²² While deadlines were set, the methods for meeting the timelines were not specified. Rather, wireless carriers, LECs and PSAPs were left to develop systems that would meet the requirements for each phase by specified dates.¹²³ The FCC determined that by remaining “technologically and competitively neutral,”¹²⁴ they would encourage parties to “arrive at a

118. Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Fifth Memorandum Opinion and Order*, 15 F.C.C.R. 22,810 para. 2 (2000).

119. 47 C.F.R. § 20.18 (2002).

120. *See e.g., First E-911 Report and Order*, *supra* note 92.

121. *See, e.g., Third E-911 Report and Order*, *supra* note 105.

122. *See First E-911 Report and Order*, *supra* note 92, paras. 61–72.

123. *Id.*

124. WIRELESS TELECOMMUNICATIONS BUREAU, FEDERAL COMMUNICATIONS COMMISSION 2004 BIENNIAL REGULATORY REVIEW §20 (2005), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-20A1.pdf [hereinafter 2004 BIENNIAL REVIEW].

solution that is both effective and cost-efficient.”¹²⁵

This attempt at partnership was abandoned, to some extent, when the first problems arose.¹²⁶ When carriers failed to meet their obligations under Phase II, the FCC used the possibility of an enforcement action to obtain consent decrees. The consent decrees bind the carriers to a revised Phase II deployment schedule and require the carriers to issue quarterly reports on their progress in meeting these goals.¹²⁷

b. The Cost-Recovery Problem

As with CALEA, the FCC made additional changes to its rules during development and deployment of the E-911 solution that arguable slowed completion of the service. One area was cost recovery. The FCC initially required that a mechanism be in place to allow wireless carriers to recover adequate costs before deploying E-911 services.¹²⁸ When the FCC reviewed its original E-911 order, it relied on the parties to the Consensus Agreement, who filed a joint status report, in assessing what progress had been made.¹²⁹ The findings of the report led the FCC to conclude, among other things, that the cost-recovery requirement was an impediment to a timely roll-out of E-911.¹³⁰ The FCC believed that removing the cost-recovery requirement was necessary to eliminate uncertainty in the market.¹³¹

The cost-recovery requirement mandated that provision of Phase I and Phase II services was preconditioned on the development of a mechanism for both wireless carriers and PSAPs to recover costs associated with deployment.¹³² The FCC maintained the cost-recovery requirement for PSAPs,¹³³ but after further review, removed the requirement as a prerequisite for wireless carrier provision of E-911 service.¹³⁴ As the FCC explained, they faced an “either/or” proposition.¹³⁵ Either they get involved

125. *Id.*

126. See *Second Report and Order*, *supra* note 92; 2004 BIENNIAL REVIEW, *supra* note 124, at §20 (“Where major carriers fell behind schedule or requested additional time, the Commission negotiated consent decrees which provided penalties for failure to comply and set specific enforceable future Phase II deployment schedules.”).

127. See *e.g.*, AT&T Wireless, *Order*, 17 F.C.C.R. 19,938 (2002); T-Mobile USA, Inc., *Order*, 18 F.C.C.R. 15,123 (2003).

128. See *First E-911 Report and Order*, *supra* note 92, paras. 85–90.

129. See, *e.g.*, *Second E-911 Report and Order*, *supra* note 95, para. 16.

130. *Id.* para. 18.

131. *Id.* paras. 43–50.

132. See *First E-911 Report and Order*, *supra* note 92, paras. 85–90.

133. See *Second E-911 Report and Order*, *supra* note 95, para. 65.

134. See *id.*

135. *Id.* para. 39 (“In order to move E-911 implementation forward, it appears that we

in regulating the specifics of a cost-recovery mechanism or they eliminate the cost-recovery mechanism in its entirety.¹³⁶ They chose elimination.

The original rules served as a guarantee to wireless carriers that they would not have to fund, or pass through to customers, significant costs associated with infrastructure investments. It was widely acknowledged that the cost-recovery requirement was intended to mimic the systems in place for wireline E-911 providers.¹³⁷ However, the FCC found that because wireless carriers are not rate-regulated¹³⁸ there was no need for cost-recovery mechanisms. This distinction was determinative in the FCC's ruling to eliminate the cost-recovery requirement. While the FCC's decision was supported by the courts,¹³⁹ the fight over cost-recovery, and other changes made by the FCC during over thirty E-911-related proceedings,¹⁴⁰ added to the uncertainty surrounding the service, and devalued the initial agreement forged between the industry, public safety, and government.

The ongoing CALEA and E-911 proceedings highlight the difficulties with trying to regulate a technical issue that originally was designed as an industry-government partnership. These proceedings also underscore the problems that develop when rules are changed during development and deployment of a service. At a minimum, this phase of public safety regulation provides an example of how even the best of regulatory intentions can hamper deployment of a service. These precedents obviously have, and will continue, to impact the approach to government intervention in homeland security and public safety proceedings, and can serve as a foundation against which all other proceedings in this area are measured.

must either adopt a much more detailed definition of a cost recovery mechanism or delete that condition from the rule.”).

136. *Id.*

137. *Id.* para. 27 (“Public Safety Associations agree with CTIA and the carriers that, as reflected in the Consensus Agreement, the parties intended to pursue publicly-adopted surcharges similar to those often used for wireline 911. . .”).

138. *Id.* para. 61. (“This is [self-recovery] the normal way that costs of doing business, including the costs of complying with government-imposed requirements, are recovered in an industry free of rate regulation.” [emphasis added]).

139. *See* U.S. Cellular Corp. v. FCC, 254 F.3d 78, 80, 89 (D.C. Cir., 2001).

140. *See, e.g.*, Letter from Thomas Sugrue, Chief, Wireless Telecommunications Bureau, to Marlys R. Davis, E-911 Program Manager, King County E-911 Program Office (May 7, 2001) (on file with Author) (responding to a request for clarification from King County, Washington, and shifting the cost responsibilities for additional facilities to wireless carriers); *see also* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Order*, 16 FCCR 18,277 (2001) (modifying requirement that PSAPs be E-911 capable as a prerequisite to a carrier's deployment obligation, effectively obligating carrier to deploy E-911 prior to the PSAP's actual readiness).

III. THE EVOLUTION FROM PUBLIC SAFETY REGULATION TO HOMELAND SECURITY REGULATION

A. Introduction

The first phase of regulation in this safety and security environment, initiated in the name of public interest and public safety, involved FCC leadership of industry toward a goal—traditional regulation. The second phase is markedly different. It has taken place in the shadow of the tragedy of 9/11. The new rationale for government involvement has been the security of the homeland, not safety of the individual, and the process has evolved toward greater industry involvement in the regulatory *outcome*, not just the development of the mandate (as occurred in the first phase). The phrase “private-public partnerships” has been adopted to describe this approach.

Three main government initiatives were launched under this partnership approach to regulation: Wireless Priority Service (“WPS”), Outage Reporting, and the Critical Infrastructure Information Act (“CIIA”). Regarding the wireless industry, the first two began as a partnership between industry and the FCC. The third, the CIIA, was enacted by Congress to provide private industry with confidence to partner and share key information with government.¹⁴¹ The Bush Administration has publicly embraced this approach to regulation, calling on industries across the country to engage in private-public partnerships with the government for the good of the country.¹⁴²

This Section traces the development of WPS, Outage Reporting, and the CIIA, and outlines the role that the Network Reliability and Interoperability Council (“NRIC”) may have played in supporting the general movement to the second phase of homeland security regulation, public-private partnerships. This section will highlight Priority Access as a notable example of what can be accomplished when industry and

141. During the debate over the CIIA, proponents of the CIIA argued that “private industry would be unwilling to voluntarily share critical infrastructure information with the federal government without assurances that its confidential business information would not be released by the government.” GINA MARIE STEVENS, CONGRESSIONAL RESEARCH SERVICE, HOMELAND SECURITY ACT OF 2002: CRITICAL INFRASTRUCTURE INFORMATION ACT CRS-2 (Report for Congress, 2003), at <http://www.fas.org/irp/crs/RL31547.pdf> [hereinafter CRITICAL INFRASTRUCTURE ACT REPORT].

142. See, e.g., Marisa Helms, *Ridge Calls for Public-private Partnerships to Improve Security*, MINNESOTA PUBLIC RADIO, June 20, 2003, at http://news.minnesota.publicradio.org/features/2003/06/20_helmsm_ridge/; see also Press Release, United States Department of Housing and Urban Development, Bush Administration Highlights Private-Public Partnership to Increase Minority Homeownership (July 9, 2002), available at <http://www.hud.gov/news/release.cfm?content=pr02-074.cfm>.

government work together. This section also will analyze the Outage Reporting proceeding and discuss why ultimately the FCC chose to mandate an outcome. Finally, this section concludes that the framework now is in place for partnerships in the name of homeland security between government and the wireless industry. Again, as at the end of the first phase, this phase ended with the question remaining as to which model government will pursue going forward, a continued migration toward private-public partnerships, or a reversion toward mandates.

B. NRIC: The Foundation for Public-private Partnerships

As the FCC moved into what the Authors of this Article are entitling the second phase of public safety-homeland security regulation, the FCC already had a successful example of a voluntary, cooperative, and beneficial public-private partnership. The NRIC, established in January 1992 as the National Reliability Council following a series of major landline service outages,¹⁴³ now is operating under its seventh charter.¹⁴⁴ Initially developed to study the causes of those outages and work to prevent their recurrence, this public-private partnership, composed of representatives from across the telecommunications industry, public safety, and the FCC, today is an integral component of the effort to secure critical infrastructure and improve homeland security.¹⁴⁵

1. NRIC's historical role in the regulatory process

The NRIC was formed to encourage cooperation among industry, consumer groups and members of academia, and to draw on these resources to help guide the FCC's role in enhancing network reliability.¹⁴⁶ Over the years, the goals of NRIC have changed, but it continues to be a successful model of what true industry-government partnerships can become. Whether the group focuses on ensuring that the country's telecommunications networks were Year 2000 ("Y2K") compliant,¹⁴⁷ or

143. See NRIC Publications, at <http://www.nric.org/pubs/index.html> (last visited May 18, 2005).

144. See NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL, CHARTER OF THE NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL - CHARTER VII (Apr. 15, 2004) available at http://www.nric.org/charter_vii/NRICVII_Charter_FINAL_Amended_2004_3_12_04.pdf [hereinafter NRIC CHARTER].

145. The NRIC is a Federal Advisory Committee to the FCC and is currently chartered to recommend to the FCC and the communications industry ways of assuring optimal reliability and interoperability of the nation's communication infrastructure. See *id.* at 1.

146. 2000 Biennial Review – Telecommunications Service Quality Reporting Requirements, *Notice of Proposed Rulemaking*, 15 F.C.C.R. 22,113, para. 40 (2000).

147. See discussion *infra* Part III.B.1.a.

developing and publishing Network Reliability Best Practices,¹⁴⁸ the NRIC has a track record of success.

a. Preparing for Year 2000

Beginning in 1998, the NRIC focused on two principle questions regarding the potential problems that could occur across telecommunications networks as the country moved into the new millennium: what is the impact of the “year 2000 problem” on telecommunications networks and services, and what is the current status of network reliability? As part of its review, the NRIC completed a survey of international telecommunications readiness covering 84 of the 225 countries throughout the world. Additionally, the NRIC cohosted a one-day Y2K contingency planning seminar that provided participants “with the concepts and tools necessary for developing operational contingency plans around the Year 2000 date change event.”¹⁴⁹

The NRIC established Focus Group One, Subcommittee 2, to pursue Y2K interoperability testing. This subcommittee assessed Y2K readiness throughout the industry, analyzed any gaps, and made recommendations. Over seventy-five companies responded to the group’s survey. By October of 1999, the NRIC declared that the telecommunications industry was rapidly becoming prepared for the Y2K conversion.¹⁵⁰ After extensive investigation, the group concluded that “the risk of failure of the domestic PSTN is minimal, and it is believed that additional testing is not warranted.”¹⁵¹

b. Securing the Reliability of Telecommunications Networks

Once again, in 2002, the NRIC addressed another difficult challenge. The task was to “facilitat[e] the reliability, robustness, security, and interoperability of public telecommunications networks.”¹⁵² Specifically, NRIC was to “prepare and provide recommended requirements for network

148. See discussion *infra* Part III.B.1.b.

149. NRIC Publications, at <http://www.nric.org/pubs/index.html> (last visited May 18, 2005).

150. See Press Release, Network Reliability and Interoperability Council, U.S. Telecommunications Industry Virtually Completes Year 2000 Readiness (Oct. 20, 1999) at <http://www.nric.org/pubs/index.html> (“[T]he U.S. Telecommunications Industry is virtually complete with its Year 2000 remediation and implementation programs and local and long distance services are expected to continue to function on and after January 1, 2000.”).

151. NRIC IV Focus Group One: Subcommittee 2, Powerpoint Presentation at the NRIC Meeting, at 18 (July 14, 1999), at <http://www.nric.org/fg/fg1/sc2/fg1-sc2-july14-presentation.ppt>.

152. See Charter of the Network Reliability and Interoperability Council–VI, at http://www.nric.org/charter_vi/index.html (last visited May 18, 2005).

reliability and network reliability measurements for wireline, wireless, satellite, and cable public telecommunications networks.” The result from NRIC was the development of over six hundred best practices across several subject matter areas. As with previous NRIC efforts, this too was a successful example of private-public partnership.

2. NRIC’s Newest Focus—Wireless

The NRIC now faces its newest challenge: wireless. That focus is evident not only in its charter but also in both its membership and leadership, as NRIC has evolved to more accurately reflect the telecommunications industry. While in the past the NRIC Board obviously contained representatives from the key wireline providers, since 1994 the group has expanded to include satellite, cable, and wireless industry leaders. The current leadership reflects this evolution. For the first time, the chairman of NRIC VII is from a wireless company. Tim Donahue, CEO of Nextel, leads a very diverse NRIC Board, including representatives from industry, state regulators and consumer groups.¹⁵³ NRIC VII’s mission is to “partner with the Federal Communications Commission, the communications industry and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices across the burgeoning telecommunications industry.”¹⁵⁴ Specifically, under its current charter,¹⁵⁵ the NRIC VII will address issues including improvement of E-911, increased deployment of broadband, and possible development of specific best practices for homeland security, wireless, and public data network services.¹⁵⁶

The NRIC’s ability to adapt to both new concerns (Y2K and homeland security) and a new telecommunications landscape (broadband, satellite, and wireless) clearly highlights its value to the constantly changing telecommunications landscape. The NRIC has demonstrated the effectiveness of the private-public partnership model time and again. The FCC need only look to the historical performance of NRIC, as well as the present significance embodied in the development of wireless-specific best practices,¹⁵⁷ to conclude that it can continue to apply this partnership model

153. See NRIC VII Members, at http://www.nric.org/charter_vii/nric_vii_org.html (last visited May 18, 2005).

154. NRIC VII Mission Statement, at <http://www.nric.org> (last visited May 18, 2005).

155. The current charter was renewed in December 2003, amended in April 2004, and runs through December 2005. NRIC CHARTER, *supra* note 144, at 9.

156. See *id.*

157. See NRIC Best Practices, at http://www.bell-labs.com/cgi-user/krauscher/bestp.pl?textsearch=&networktype=wireless&operator=AND&kw_1=&kw_2=&kw_3=&fieldList= (last visited May 18, 2005).

to the growing CMRS industry.

C. *Critical Infrastructure Information Act—Building the Foundation for Partnership*

1. Creation of the Act

The passage of the CIIA¹⁵⁸ was yet another confirmation that both Congress and the Bush Administration recognized the importance of private industry partnering with government.¹⁵⁹ The Act, passed as part of the larger Homeland Security Act, insures that voluntarily submitted¹⁶⁰ information about the country's critical infrastructure would be exempted from public disclosure.¹⁶¹ It reinforces government's desire to partner voluntarily with industry, as the data submitted to government must be submitted voluntarily to be eligible for CIIA protection. For wireless carriers, the passage of the CIIA allows the industry to share information with government officials without the fear of negative publicity, civil liability, and the possibility that the information will be used by competitors. The importance of that infrastructure, particularly the telecommunications infrastructure, was demonstrated on 9/11.¹⁶² With approximately 85 percent of the country's infrastructure controlled by private industry,¹⁶³ it is essential that government work with private industry on its protection. Accordingly, Congress and the Bush Administration set out to create incentives for industries to voluntarily submit information on the nation's critical infrastructure. Proponents of the CIIA argued that "private industry would be unwilling to voluntarily share critical infrastructure information with the federal government without assurances that its confidential

158. See Homeland Security Act of 2002, 6 U.S.C. § 131–133 (Supp. 2002).

159. See NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 397–398 (2004), available at <http://www.9-11commission.gov/report/index.htm> [hereinafter 9/11 COMMISSION REPORT] ("The [Department of Homeland Security] is also responsible for working with the private sector to ensure preparedness . . . [H]omeland security and national preparedness therefore often begins with the private sector.").

160. "Information sharing between public and private entities about threats and vulnerabilities to critical infrastructures was a central component of the President's proposal." CRITICAL INFRASTRUCTURE ACT REPORT, *supra* note 141, at 1.

161. Homeland Security Act of 2002, 6 U.S.C. § 131(2) (Supp. 2002) (protecting data "that is voluntarily submitted to a covered Federal agency").

162. See New Part 4 of the Commission's Rules Concerning Disruptions to Communications, *Report and Order and Further Notice of Proposed Rule Making*, 19 F.C.C.R. 16,830, para. 16 (2004) [hereinafter *Outage Reporting Order and FNPRM*].

163. See 9/11 COMMISSION REPORT, *supra* note 159, at 398.

business information would not be released by the government.”¹⁶⁴ The result is a carefully worded Act that facilitates the creation of private-public partnerships and the sharing of information that otherwise would not be available to government.

2. Facilitating Information Sharing

To some, the CIIA is necessary to ensure private-public cooperation,¹⁶⁵ to others it is a carve-out from civil liability.¹⁶⁶ Those opposed to the CIIA stated that the Freedom of Information Act (“FOIA”) Exemption 4¹⁶⁷ already grants similar protection to information about critical infrastructure voluntarily shared with the government.¹⁶⁸ There are, however, nuanced, but very critical, differences between CIIA and FOIA Exemption 4. Primarily, the differences involve both the threat of criminal penalties¹⁶⁹ and the *presumption* that information under CIIA *should not* be released to the public.¹⁷⁰ The CIIA “eliminates the presumptive right of access by any person—corporate or individual, regardless of nationality—to existing, unpublished, Department of Homeland Security (“DHS”) records on critical infrastructure information. [The CIIA] leaves no discretion.”¹⁷¹ These limitations shift the risk to government to ensure that such data never is released.

There are several elements of the CIIA that may comfort private industry as it considers partnering with government, possibly on critical infrastructure protection. First, “Critical Infrastructure” is defined as, “any information not customarily in the public domain and related to the security

164. CRITICAL INFRASTRUCTURE ACT REPORT, *supra* note 141, at CRS-2.

165. *Id.* During the debate over the CIIA, proponents of the CIIA argued that “private industry would be unwilling to voluntarily share critical infrastructure information with the federal government without assurances that its confidential business information would not be released by the government.” *Id.*

166. See Rena Steinzor, “*Democracies Die Behind Closed Doors*”: The Homeland Security Act and Corporate Accountability, 12 Kan. J.L. & Pub. Pol’y 641 (2003) [hereinafter *Democracies Die*].

167. See *id.* See also *Securing Our Infrastructure: Public-private Information Sharing: Hearing Before the Senate Comm. on Governmental Affairs*, 107th Cong. (2002) (statement of David L. Sobel, General Council, Electronic Privacy Information Center), available at http://www.senate.gov/%7Egov_affairs/050802sobel.htm.

168. See *Outage Reporting Order and FNPRM*, *supra* note 162, paras. 42–46.

169. Homeland Security Act of 2002, 6 U.S.C. § 133(f) (Supp. 2002).

170. See *Democracies Die*, *supra* note 166, at 654 (discussing the need under FOIA Exemption 4 for the government to show that information should not be released, compared to the need under CIIA for the public to show that information does not fit into protected status).

171. CRITICAL INFRASTRUCTURE ACT REPORT, *supra* note 141, at CRS-6.

of critical infrastructure of protected systems.”¹⁷² Voluntary is defined by CIIA as the submission of critical infrastructure information “in the absence of . . . [an] agency’s exercise of legal authority to compel access to or submission of such information.”¹⁷³ These broad definitions provide government with an opportunity to protect from FOIA disclosure data received as part of a voluntary public-private partnership.¹⁷⁴

Second, while “voluntary” and “critical infrastructure information” are defined under CIIA, the responsibility for determining the procedure for receipt, care and storage” of the voluntary critical infrastructure information lies with the DHS.¹⁷⁵ The CIIA stipulates that DHS must acknowledge “receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government.”¹⁷⁶ This DHS determination is the final element in securing a confidential flow of voluntary information from industry to government. This is so because DHS, the agency responsible for securing the nation’s critical infrastructure,¹⁷⁷ has a vested interest in the continuous flow of information regarding communications facilities. This process, as explained in section 133 of CIIA, confirms the goal of facilitating partnerships.

D. Reporting Wireless Network Outages

In spite of the passage of the CIIA, the FCC in early 2004 adopted an Order requiring segments of the telecommunications industry, including wireless, to provide data on network outages. As in the areas of E-911 and CALEA, this requirement initially existed only in the landline environment.¹⁷⁸ Neither satellite nor wireless carriers were subject to the FCC’s initial service outage reporting rules. In the August 4th Report and Order, the FCC expanded this requirement to all communications providers of voice and/or paging services (cable, satellite,

172. Homeland Security Act of 2002, 6 U.S.C. § 131(3) (Supp. 2002).

173. *Id.* § 131(7)(A).

174. CIIA also adds additional exemptions. The submitted information is exempt from traditional *ex parte* rules of disclosure, as well as exempt from use in civil lawsuits so long as the information is submitted in good faith. The information may be disclosed to Congress and the GAO or “in furtherance of an investigation or the prosecution of a criminal act,” but otherwise it remains protected. *See id.* § 133(a)(1)(B)–(D).

175. *Id.* § 133(e)(1).

176. *Id.* § 133(e)(1)(A).

177. Press Release, Office of the Press Secretary, The White House, Homeland Security Presidential Directive 7 (Dec. 17, 2003), at <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html> [hereinafter HSPD 7].

178. Section 63.100 of the Commission’s rules requires telecommunications carriers, other than cellular and satellite carriers, to report significant service disruptions. 47 C.F.R. § 63.100 (1992).

wireless, and wireline carriers are now subject to outage reporting requirements).¹⁷⁹

For the wireless industry, this proceeding began as a voluntary partnership between industry and government. It continued the movement to partnership began in Phase II. However, while the FCC initially offered several industries, including the wireless industry, the opportunity to provide the data voluntarily, ultimately the FCC decided to require the data. The FCC stated that it had charged the industries not subject to the existing mandatory reporting rules to provide information voluntarily.¹⁸⁰ According to the FCC, the efforts of those industries, including wireless, fell short of expectations.¹⁸¹ The FCC believed that it had “a history of several years of unsuccessful voluntary outage reporting trials” conducted over a four-year period under a process designed by carriers.¹⁸² Although the FCC had “encouraged telecommunications providers to participate actively and fully in these network outage-reporting efforts, [it] observed that participation was spotty and that the quality of information obtained was very poor.”¹⁸³

Accordingly, the FCC stopped partnering with industry and initiated a proceeding to establish a mandate. Mandating reporting of this information had a significant impact on the wireless industry. First, the industry lost the opportunity to work with government on a voluntary basis. Second, by *requiring* data collection, the information automatically would fall outside of the CIIA.

Fortunately for the wireless industry, the FCC ultimately concluded that data received as part of this requirement should be protected from public disclosure.¹⁸⁴ In the proceeding, the FCC received comments from across industry and from the DHS on a desire to protect this information from disclosure. Ultimately, the FCC concluded that it would gather this critical infrastructure information and then securely transmit it to DHS.¹⁸⁵ The FCC stated that this information would be protected in one of three

179. *Outage Reporting Order and FNPRM*, *supra* note 162, paras. 97–114 (2004). Essentially, the FCC mandated that all carriers must disclose network outages when thirty minutes of downtime occurs or when 900,000 user minutes are potentially affected. *Id.* para. 97.

180. *Id.* para. 18.

181. *Id.* (stating that “[t]he results of this effort, as of the date of adoption of the *Notice*, had not provided us with the quality or quantity of information that we need to accurately monitor the health of the Nation’s telecommunications infrastructure. . .”).

182. *Id.* para. 37.

183. *Id.* (citation omitted).

184. *See id.* para. 3.

185. *See id.* para 47.

ways: that it will be covered under CIIA, that it will be covered under FOIA Exemption 4,¹⁸⁶ or that the FCC is required under the Homeland Security Presidential Directive-7 to protect the sensitive information.¹⁸⁷

Leading up to the FCC's adoption of the Order, the industry had worked to secure a voluntary disclosure of the information, hoping to provide the data under the protection of the CIIA.¹⁸⁸ While the ultimate outcome of the proceeding was not a voluntary effort, as many in the wireless industry had requested, consistent with Phase II of homeland security regulation, the telecommunication industries had an opportunity to provide the data voluntarily before the FCC ultimately mandated the reporting. Additionally, after deciding to mandate outage reporting, the FCC did work with industry on many of the elements of concern. While not a perfect outcome for the wireless industry, this proceeding confirmed that the FCC would continue to consider private-public partnerships as a way of achieving its goals.

E. Wireless Priority Service: the Prototype of the Partnership Model

While NRIC provides an historical example of a private-public partnership in telecommunications, and the CIIA facilitates partnerships going forward, WPS is the wireless industry's model of successful industry-government partnership. The rapid deployment of this service on the wireless network is a testament to what can happen when a coordinated government effort meets a motivated industry. From the Bush Administration's request for an initial priority service shortly after 9/11, to the deployment nationwide of WPS today, government never proposed a mandate and always worked with industry toward a voluntary solution.

The model utilized in this proceeding was to simply establish the ground rules,¹⁸⁹ facilitate and fund development, and then allow industry experts to develop the solution. Government likely recognized that a true

186. Particularly if it is information that, if disclosed, would put the carrier at a competitive disadvantage. *See id.* paras. 42–46.

187. *See id.* para. 41; HSPD 7, *supra* note 177.

188. Wireless carriers expressed their belief that a voluntary system outage reporting system, the Industry-Led Outage Reporting Initiative (“ILORI”), was preferable to mandatory system outage reporting because they could report to the FCC and DHS simultaneously and there would be no issue as to whether the reporting was voluntary under CIIA. *See, e.g., Outage Reporting Order and FNPRM, supra* note 162, paras. 42–46.

189. *See, e.g.,* 47 C.F.R. § 64.402 (2002) (stating that “[c]ommercial mobile radio service providers that elect to provide priority access service to National Security and Emergency Preparedness personnel shall provide priority access service in accordance with the policies and procedures set forth in Appendix B to this part.”).

understanding of what the industry could do, and when it could be done, would only accurately come from industry. The result is a public-private partnership that resulted in a fully functioning service developed in an extremely short timeframe.

1. The Call for Wireless Priority Service

As with other services or requirements in this field of public safety (Phase I) and homeland security (Phase II), WPS has its origins in landline telecommunications. The Government Emergency Telecommunications System ("GETS") was designed to provide National Security and Emergency Preparedness ("NSEP") personnel with priority over other landline traffic in the event of an emergency.¹⁹⁰ GETS was developed using existing features of the landline networks.¹⁹¹ While GETS-eligible callers receive a priority within the queue, they do not preempt any calls.

WPS is similar to the GETS program in several ways. Like GETS, WPS enables certain NSEP personnel to obtain a priority for the next available radio channel when necessary to initiate emergency calls.¹⁹² Also like GETS, WPS does not preempt calls in progress. Under WPS, authorized users activate the feature on a per-call basis by dialing a feature code such as *XX.¹⁹³ Callers are given a priority of one through five based on their NSEP designation, and those users are provided access to CMRS channels before any other CMRS callers.¹⁹⁴ WPS "is to be available to authorized NSEP users at all times in equipped CMRS markets where the service provider has voluntarily decided to provide such service."¹⁹⁵

The most notable differences between WPS and GETS are the event that accelerated WPS deployment and the process by which it was developed. While, as discussed above, WPS shares some similarities with the GETS program, the wireless service is different in that at its core, the service is "an *enhancement* to basic cellular service."¹⁹⁶ This fact alone separates WPS from GETS. Because it was not a basic element of wireless

190. Government Emergency Telecommunications Service (GETS), at http://www.atis.org/tg2k/_government_emergency_telecommunications_service.html (last modified Feb. 28, 2001).

191. *Id.*

192. See Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Through the Year 2010, *Second Report and Order*, 15 F.C.C.R. 16,720, 16,722, para. 5 (2000) [hereinafter *Public Safety Second Order*].

193. 47 C.F.R. pt. 64, app. B, at 2.c. (2002).

194. *Id.*

195. *Id.*

196. Wireless Priority Service, at <http://wps.ncs.gov> (last visited May 18, 2005).

service, WPS required an action to initiate development and ensure that there would be continued focus on deployment. The tragedy of 9/11 provided such an action-forcing event.

While discussions of a wireless priority access service began in the early 1990's, it was not until after 9/11 that government began to request development of the service. In fact, while the FCC issued a decision to "allow commercial mobile radio service to offer Priority Access Service (PAS) to public safety personnel at the Federal, State and local levels to help meet the national security and emergency preparedness (NSEP) needs of the Nation"¹⁹⁷ in July of 2000, it was not until after 9/11 that government's efforts to develop the service accelerated. The National Security Council, "[r]eacting to the events of 9/11, [issued] guidance to the National Communications System" to "move forward" on an immediate wireless priority access solution for the Washington, D.C. market. The target for such a solution would be sixty days.¹⁹⁸

In parallel, the National Communications System ("NCS") was tasked with developing a nationwide solution within one year.¹⁹⁹ With these tight deadlines, government easily could have mandated a solution. Instead, this request from the National Security Council initiated a two-phase development effort. The first phase involved the use of "commercially available and readily implemented technology for limited geographic areas." The second was "geared to the development of a long-term, nationally available solution."²⁰⁰

2. Partnering for Success—Waivers, Liability Protection, and Funding

Prior to development and deployment of a successful WPS, several elements of the regulatory puzzle had to be addressed. While the National Security Agency was calling for the rapid development of WPS, the FCC already had completed some of the important groundwork for development of the service. First, the FCC determined that it was not going to mandate a solution. Second, guidelines were established that would form the basis for developing a solution. Third, the development was funded.

197. Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communications Requirements Through the Year 2010 Establishment of Rules and Requirements for Priority Access Service, *Second Report and Order*, 15 F.C.C.R. 16,720 (2000) [hereinafter *Priority Access Second Report and Order*].

198. See Wireless Priority Service, Program Information, at http://wps.ncs.gov/program_info.html (last visited May 18, 2005).

199. *Id.*

200. *Id.*

The process began at the FCC in 2000. In a 2000 Report and Order, the FCC set the stage for a voluntary service when it stated that it would “permit, but not require, commercial mobile radio service (CMRS) providers to offer [WPS] to NSEP personnel.”²⁰¹ That first element of the decision, the conclusion that the service would not be mandated, made possible a partnership between industry and government.

Next, the FCC addressed some concerns raised by NCS about development of the service. NCS had argued that the service “had not been fully developed precisely because the FCC had not yet established operating protocols for PAS. Once the manufacturers know the protocols they need to support, or the standards to which they need to adhere, NCS contends the manufacturers will act accordingly.”²⁰² The FCC directly addressed this concern. It concluded that if a carrier

choose[s] to offer PAS, we are requiring them to adhere to uniform operating protocols concerning the number of priority levels and the priority level for particular NSEP users. We believe that uniform operating protocols will: (a) ensure the compatibility of a peacetime PAS system with a wartime system; (b) allow federal and out-of-region NSEP personnel to avail themselves of PAS; and (c) enable a PAS system to be far more effective. In addition, we conclude that: (a) PAS will include five priority levels, with non-government NSEP personnel receiving entitlement to a priority level as appropriate; (b) access to PAS should be limited to key personnel and those with leadership responsibilities; and (c) the National Communications System (NCS) will have responsibility for the day-to-day administration of PAS, with oversight responsibilities residing with the Commission.²⁰³

The FCC also addressed several very important issues that likely contributed to rapid development and deployment of the service. First, the FCC did not “require carriers to adhere to particular technical standards to implement PAS.” As the industry was composed of multiple carriers providing services on varied platforms, mandating a specific technical standard could actually slow development. Additionally, the FCC chose not to require a portion of a carrier’s network to be set aside for WPS use.²⁰⁴

The FCC also addressed the difficult issue of liability. The FCC

201. *Priority Access Service Second Report and Order*, *supra* note 197, para. 3.

202. *Id.* para. 13.

203. *Id.* para. 4.

204. *Id.* para. 18.

Some parties comment that carriers offering PAS should be free to limit the amount of spectrum they make available to PAS so that non-priority users will be able to access the network. Since PAS will be a voluntary service of CMRS systems, and since we do not know the extent of the demand for PAS by NSEP personnel, we will permit carriers to limit PAS to a portion of their spectrum.

Id.

concluded that “a carrier’s provision of PAS in accordance with our Rules will be prima facie lawful under federal law, thereby imposing a heavy burden on any complainant who claims a violation of the Communications Act, in particular, a violation of Section 202’s anti-discrimination provisions.”²⁰⁵ The FCC concluded that “without such protection from liability, we believe that carriers are unlikely to offer [WPS].”²⁰⁶

3. Deployment

With the foundation work completed by the FCC in 2000, and guidance from the Bush Administration in October 2001, the NCS looked to begin immediate initiation of service for the Washington metropolitan area and looked to secure service both for New York City and Utah.²⁰⁷ Once again, the FCC acted to facilitate the service. In November of 2001, VoiceStream Wireless Corporation (now T-Mobile) filed a request with the FCC seeking a waiver of the rules to provide a wireless priority service to the NCS.²⁰⁸ This waiver was supported by the NCS, and was required because T-Mobile’s proposed service did not initially conform to the Report and Order requirement to invoke the priority service on a call-by-call basis.²⁰⁹ Instead of forcing compliance with the established guideline, the FCC adopted a Memorandum, Opinion and Order granting the waiver request.²¹⁰

With the waiver secured, the NCS entered into subcontracts with the two initial WPS service providers, VoiceStream (now T-Mobile) and Globalstar.²¹¹ T-Mobile’s implementation of the immediate solution became

205. *Id.* para. 4.

206. *Id.*

207. Wireless Priority Service, Program Information, at http://wps.ncs.gov/program_info.html (last visited May 18, 2005).

208. Petition for Partial Waiver of Section 64.402 of the Commission’s Rules, *Petition for Partial Waiver*, WT Dkt. No. 01-333 (2001) (filed by VoiceStream Wireless Corp.).

209. See VoiceStream Petition for Waiver of Section 64.402 of the Commission’s Rules, *Statement in Support of Petition for Waiver*, WT Dkt. No. 01-333 (2001) (filed on behalf of the National Communications System). The NCS is an organization created by Executive Order to administer and manage the telecommunications assets of twenty-three federal government organizations in serving the national security and emergency preparedness (“NSEP”) needs of the federal, state and local governments. See Exec. Order No. 12,472, 49 Fed. Reg. 13,471 (Apr. 3, 1984). VoiceStream Wireless Corporation, *Memorandum Opinion and Order*, 17 F.C.C.R. 6134, para. 1 n.3 (2002) [hereinafter *VoiceStream Order*].

210. *VoiceStream Order*, *supra* note 209.

211. The NCS provided Globalstar satellite phones to quickly field the immediate WPS in the Salt Lake City area during the Olympics for over 600 users. Globalstar increased satellite capacity and redirected Utah calls directly to a US-based earth station. Globalstar also increased landline trunking at the earth station for GETS calls. See Wireless Priority Service, at <http://wps.ncs.gov> (last visited May 18, 2005).

operational during May 2002 in Washington and New York. By November 2002, T-Mobile supported 2084 WPS users in Washington and 725 in New York, for a total of 2809 WPS wireless users.²¹²

4. Exporting the Partnership Model

The decisions by the FCC, the DHS, and Congress to allow the wireless industry to develop and deploy a WPS solution accelerated its deployment. Quick action, and inaction, by the FCC, combined with successful stewardship of the development process by DHS, resulted in rapid roll-out of an operational system. The service now is being offered by three CMRS carriers (T-Mobile, Cingular, and Nextel) that provide service throughout the country.²¹³ That effort continues as the NCS works toward deploying the service across the CDMA platform. As of December 2004, there were over 11,000 WPS users, with the goal of expanding to 200,000 GSM users and 150,000 CDMA users.²¹⁴

F. *The Legacy of the Second Phase of Homeland Security Regulation*

Despite the final outcome of the Outage Reporting proceeding, the framework now is in place for private-public partnerships in the name of homeland security between government and the wireless industry. The Outage Reporting Order is an illustration that the FCC will mandate regulation if it believes that industry is not proceeding quickly under a voluntary regime. In the case of Outage Reporting, it was not the process of partnering that was broken, but rather that particular partnering process. The FCC believed that the industry did not do enough to warrant a voluntary approach.

Alternatively, the FCC has two precedents with which it is intimately familiar where partnerships with industry clearly have been beneficial—NRIC and WPS. Comparing those two successes with the recent history of Outage Reporting and the long-term implementation issues surrounding E-911 and CALEA, the industry's incentive to partner is strong. The key question is which path of homeland security regulation will the government, particularly the FCC, employ going forward?

212. *Id.*

213. See Press Release, National Communications System, NCS Begins Deployment of Nationwide Wireless Priority Service (Jan. 21, 2003), available at <http://wps.ncs.gov/documents/NCS%20Begins%20Deployment%20of%20Nationwide%20WPS.pdf>.

214. See Wireless Priority Service, <http://wps.ncs.gov> (last visited May 18, 2005).

IV. PHASE III: IN THE NAME OF HOMELAND SECURITY—TO PARTNER OR NOT?

A third phase of homeland security regulation has begun. As government addresses issues such as Emergency Alerts²¹⁵ and protection of critical infrastructure, the key question remains—which regulatory model government will utilize. At the intersection of homeland security and wireless, the best result is likely to come from partnering with industry. To use the first phase of public safety regulation, where the ultimate end-point was regulation, could lead to a duplication of E-911 and CALEA. Use of a modified second phase approach, such as in Outage Reporting, likely also will not result in the best outcome for the FCC, industry, or the American public. Alternatively, addressing these new issues through a cooperative and voluntary government initiative could result in the type of creative and timely thinking and development found in both the WPS proceeding and throughout NRIC.

This perspective was reflected in multiple comments to the FCC's recently released Notice of Proposed Rulemaking on the Emergency Alert System ("EAS").²¹⁶ In the NPRM, the FCC questioned whether the EAS was outdated because it relied "almost exclusively on delivery through analog radio and television broadcast stations and cable systems."²¹⁷ The FCC in fact asked whether there should be a "concerted *industry-government effort* to combine EAS with alternative public alert and warning systems."²¹⁸ T-Mobile, Nortel, and others supported the idea of a government-industry partnership.²¹⁹

As the comments highlight, a collaborative industry-government approach makes particular sense with regard to the wireless industry. During the last five years, there has been a steady wave of technological change. The industry has moved from TDMA to CDMA, GSM, and iDEN, and has utilized, or will utilize, technologies including 1xRTT, UMTS,

215. See Review of the Emergency Alert System, *Notice of Proposed Rulemaking*, 19 F.C.C.R. 15,775 (2004) [hereinafter *Emergency Alert System NPRM*].

216. See Review of the Emergency Alert System, *Reply Comments of T-Mobile USA*, EB Dkt. 04-296, at 1–2 (Nov. 24, 2004) [hereinafter *T-Mobile Reply Comments*] (stating that "as the FCC considers how to address EAS, it should allow carriers the flexibility to develop solutions and technology in cooperation with the relevant government agencies."); Review of the Emergency Alert System, *Reply Comments of Nortel*, EB Dkt. 04-296, at 3 (Nov. 29, 2004) [hereinafter *Nortel Reply Comments*] (suggesting that an industry/government forum be established to begin to investigate a definition of EAS.).

217. *Emergency Alert System NPRM*, *supra* note 215, para. 32.

218. *Id.*

219. See generally *T-Mobile Reply Comments*, *supra* note 216; *Nortel Reply Comments*, *supra* note 216.

IxEVDO, GPRS, EDGE, UMTS, and WCDMA to deliver voice and data over the wireless networks. The continued evolution of the wireless network makes engineering new government requests into existing services, without disturbing those existing services, extremely difficult.

The same issues exist regarding the protection of critical infrastructure. Government is calling on private industry to identify key assets, assess vulnerabilities, and prioritize assets to guide effective protection programs.²²⁰ The goal is to reduce vulnerability, deter threats, and minimize consequences of attacks.²²¹ Who better to inform those efforts and achieve those goals than industry. Obviously no one knows the integral elements of a wireless network better than its engineers. To ask government to identify what is a priority within an individual private company is extraordinarily difficult. The DHS recognized this and calls for an integrated effort across government and including private sector owners.²²²

In both of these proceedings, government calls for a concerted or integrated effort with industry. In both cases, industry is working voluntarily with government to address the concerns highlighted in the FCC's NPRM and DHS's Interim NIPP. Government has yet to determine whether it will establish a mandate in either of these proceedings, but at least initially it is asking questions and seeking comments as if partnership is the goal. Depending on industry efforts and government response, the third phase of homeland security regulation is beginning to resemble a true partnership between government and industry.

V. CONCLUSION

The future obviously only holds more changes for the wireless industry. When the CALEA and E-911 proceedings began over ten years ago, no one in government could have predicted where the industry would be today. As the FCC considers alerts to mobile handsets of wireless subscribers, the regulatory choice should be simple. The same is true regarding the protection of critical infrastructure. As evidenced by the WPS program, the partnership approach likely is far superior to address homeland security issues than the command and control models employed in both E-911 and CALEA. Going forward, any government effort that can be accomplished with the full support of industry through voluntary

220. See DEPARTMENT OF HOMELAND SECURITY, INTERIM NATIONAL INFRASTRUCTURE PROTECTION PLAN 2 (2005), available at <http://www.deq.state.mi.us/documents/deq-wb-wws-interim-nipp.pdf>.

221. See *id.* at 1.

222. See *id.*

industry-government partnerships should be handled as such.

