

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

In the Matters of:)	
)	
International Comparisons and Consumer)	
Survey Requirements in the Broadband)	GN Docket No. 09-47
Data Improvement Act)	
)	
A National Broadband Plan for Our Future)	GN Docket No. 09-51
)	
Inquiry Concerning the Deployment of)	
Advanced Telecommunications Capability)	
to All Americans in a Reasonable and timely)	
Fashion, and Possible Steps to Accelerate)	GN Docket No. 09-137
Such Deployment Pursuant to Section 706)	
of the Telecommunications Act of 1996,)	
As Amended by the Broadband Data)	
Improvement Act)	

Comments of L.Robert Kimball and Associates on NBP Public Notice #8

L. Robert Kimball and Associates, Inc. (“Kimball”) of Ebensburg, Pennsylvania hereby submits comments in response to the FCC’s September 28, 2009 Public Notice seeking additional comment on public safety, homeland security, and cyber security elements of National Broadband Plan.

Kimball is one of the nation’s largest engineering/architecture/consulting firms, annually ranked among the top 200 A/E firms and the top 25 telecommunications firms by Engineering News Record. Kimball’s Telecommunications & Technology Division has offered public safety and mission critical consulting services for more than 15 years. Our telecommunications and technology practice is focused on all facets of public safety, supporting operations and technologies, 911 network and call delivery, 911 call answering/tracking, radio communications cyber security and public policy.

Introduction

In considering our response, we observe that the Commission categorized its questions Public Notice #8 as though cyber security and Next Generation 911 (NG911) were separate and discrete topics. As a result, there are at least two unasked questions that should be answered in order to provide the Commission with as complete a record as possible about the unique cyber security needs of NG911. Those questions are:

- Have cyber security standards for NG911 been completely defined? If not, what has been done and what remains outstanding?
- How will small and medium sized 911 public safety answering points (PSAPs) fund cyber security initiatives necessary to connect to the broadband networks that will form the Emergency Services IP Network (ESInet)¹ basis of NG911?

Our comments in response to the Commission's NG911 questions are framed to answer two of them from a cyber security perspective.

2. **Next Generation 911 (NG911).** The Broadband Plan NOI has also been exploring whether the American public could use broadband technologies to better communicate with emergency responders when they make 9-1-1 calls.
 - a. What are the broadband infrastructure requirements necessary to support deployment of NG 911 capability?

The public safety industry is currently undergoing radical changes, made necessary by the increasingly complex and advanced communication technologies that our citizens use on a daily basis. These changes, once made, will significantly enhance public safety's ability to continue the important task of saving lives. NG911 capability is predicated on the preexistence

¹ As defined by the National Emergency Number Association in its Master Glossary of 9-1-1 Terminology NENA-00-001Version 12, July 15, 2009, ESInet means "an IP-based inter-network (network of networks) shared by all agencies which may be involved in any emergency."

of an ESInet backbone. 911 PSAPs will become interconnected through these ESInets. These networks, necessary for PSAPs and the broader emergency response community to fully realize the benefits of NG911, dramatically increase the need to ensure that comprehensive and holistic cyber security countermeasures are implemented in a consistent and meaningful manner—something not historically done within the public safety industry. The risk of cyber security attacks on the nation’s public safety infrastructure is increased with the evolution towards NG911.

- b. Have NG911 technical standards been completely defined? If not, what has been done and what remains outstanding? Where is the associated equipment in the development pipeline?

NG911 cyber security standards have not been completely defined. The National Emergency Number Association (NENA), a standards organization within the public safety industry, is in the final stages of releasing the 911 industry’s first comprehensive cyber security standards. These standards, known as “NG-SEC”, or “Next-Generation 9-1-1 Security” will apply to all entities who participate in NG911, including, but not limited to: PSAPs, vendors, telecommunications companies, service providers, content providers and any other NG911 participant. The NG-SEC standards will likely be officially published by the end of 2009 or early 2010.

In order to provide consistency, uniformity and effective security across the public safety industry, the national broadband plan should take into account the NENA cyber security standards and should do the following:

- Ensure that FCC initiatives regarding Cyber Security are in sync with the security initiatives of NENA’s Security Working Group and the NG-SEC standard.

- Broadband service providers offering solutions involving NG911 should be required to comply with the applicable portion of the NENA cyber security standards including achievement of “NG-SEC” certification.

The adoption of the aforementioned proposals will help reduce confusion, ensure consistency of application and most importantly improve cyber security within the public safety industry in concert with initiatives currently underway.

Conclusion

The release of the NG-SEC standards or any other cyber security initiative within the industry, including those brought about by the national broadband plan, will present a challenging question to the industry, particularly the PSAPs:

How will we fund the significant and costly activities necessary to ensure that the Cyber Security levels of these mission critical networks, including broadband, and that our society depends on in time of need are met and maintained?

Current funding mechanisms do not explicitly account for these new and necessary requirements. Local and state 91-1 budgets would need to be expanded to include things like hiring or outsourcing cyber security staff, or introducing basic security countermeasures like firewalls, patch management solutions, vulnerability assessments, etc. There is an open question about whether the industry would be less likely to implement these standards without an effective means to fund them. Finally, there is a vitally important question that impacts our homeland security: If there is no standardized and mandated requirement for cyber security, how would a PSAP be able to interoperate with federal agencies like the Department of Homeland Security, the Federal Emergency Management Agency (FEMA), the National Guard and more

during a time of crisis? What will be the ramifications of a failure to fund and implement these critical cyber security measures?

These questions serve as an important call to action for federal, state and local governments to actively and forcefully address the funding issue. Broadband initiatives aimed at increasing the effectiveness of public safety capabilities must include funding mechanisms specifically for cyber security. Funding explicitly targeted for *cyber security in a Next Generation 911 environment* is a necessary and important component to the overall success of our nation's NG911 efforts, without which our public safety infrastructure will be highly susceptible to the cyber risks that come with NG911. That is simply not tenable.