

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

In the Matter of)	
)	
Unlicensed Operation in the TV Broadcast Bands)	ET Docket No. 04-186
)	
Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band)	ET Docket No. 02-380
)	

PETITION FOR RECONSIDERATION

The National Cable & Telecommunications Association (“NCTA”),¹ pursuant to section 1.429 of the Commission’s rules, hereby petitions the Commission to reconsider its *Second Memorandum Opinion and Order* issued in the above-captioned proceedings.² While NCTA’s members remain concerned about the potential for interference to cable services in the home and to wireless microphone operations,³ this Petition has a narrower focus. Specifically, NCTA requests that the Commission reconsider its decision to make all information in the TV bands device database publicly available for unrestricted public browsing, including information identifying the precise geographic coordinates of cable headends and tower receive sites which

¹ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation’s cable television households and more than 200 cable program networks. The cable industry is the nation’s largest provider of broadband service after investing over \$170 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 23 million customers.

² *Unlicensed Operation in the TV Broadcast Bands; Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band*, Second Memorandum Opinion and Order, FCC 10-174 (rel. Sept. 23, 2010) (the “*White Spaces Order*” or “*Order*”).

³ *Unlicensed Operation in the TV Broadcast Bands; Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band*, ET Docket Nos. 04-186, 02-380, *see e.g.* NCTA Reply Comments on Petitions for Reconsideration, May 18, 2009; NCTA Comments on Petitions for Reconsideration, May 8, 2009; NCTA Petition for Reconsideration and Clarification, Mar. 19, 2009; NCTA Ex Parte, Oct. 27, 2008; NCTA Comments, Aug. 15, 2007; NCTA Reply Comments, Mar. 2, 2007; NCTA Comments, Jan. 31, 2007.

are sensitive, critical infrastructure for broadband Internet, voice over IP, emergency alert messaging and other critical communications services.

I. THE ORDER’S LACK OF SUFFICIENT SECURITY MEASURES WOULD ENDANGER CRITICAL INFRASTRUCTURE FOR BROADBAND INTERNET, VOICE OVER IP, EMERGENCY ALERT MESSAGING AND OTHER CRITICAL COMMUNICATIONS SERVICES

The *White Spaces Order* requires TV band database administrators to adopt reasonable and reliable security measures “to protect the contents of databases and communications between databases and TV bands devices or other databases.”⁴ The primary concerns expressed by the Commission were: (1) protecting the database from unauthorized alteration, to assure that TV band devices were receiving valid and accurate information; (2) assuring that only approved and compliant devices receive information from the database; and (3) protecting against corruption or unauthorized modification of data in transit between the database and devices.⁵

The Commission did not adopt any similar protection regarding access to the contents of the databases. To the contrary, the *Order* contemplates easy, unlimited access to all database information to facilitate “the detection and correction of errors,” and to “assist parties in locating the source of any interference that occurs and contacting the device operator to correct it.”⁶

In doing so, the Commission apparently failed to recognize the danger to the public that could arise from unfettered access to certain database information, such as the precise geographic coordinates of cable headends and their associated broadcast receive antenna specifications.⁷

These facilities are critical infrastructure for broadband Internet, voice over IP, emergency alert

⁴ *White Spaces Order* ¶ 97.

⁵ *White Spaces Order* ¶ 98-99.

⁶ *White Spaces Order* ¶ 119.

⁷ Under the *Order*, cable headends that lie beyond the protected contours of broadcast stations (as many do) may register with the database, providing their precise geographic coordinates.

messaging and other critical communications services. The headend is the point of origination and processing for most of the signals received by cable operators from external content providers, local exchange carriers, the Internet, and other networks. The headend processes and combines signals for distribution to hubs or directly to consumers. In most cases, the headend also serves as a distribution hub for the fiber nodes closest to the headend.

The *Order* would deliver this sensitive headend and tower information in a readily-accessible format, available online worldwide on an anonymous basis, to anyone who wants to see it for any purpose – including terrorists and saboteurs.

The *Order* analogized the database protections it did adopt to those used by online financial transactions.⁸ But, as the Commission noted, online financial databases are also designed with “security measures to protect against unauthorized viewing ... to ensure that only authorized users have access to information.”⁹ Similar measures are needed here to assure that sensitive database information is only accessible by parties that should be authorized to receive it. As discussed in Section II, it would be inconsistent with Commission and federal policy to undermine the security of this critical communications infrastructure by exposing such information unnecessarily. Fortunately, as discussed in Section III, the Commission can adopt straightforward security measures and still accomplish its intended purposes.

⁸ *White Spaces Order* ¶ 97 (“[V]irtually all online transactions involving financial or other confidential information currently use security measures to protect against unauthorized viewing and/or alteration of information being sent and to ensure that only authorized users have access to information.”).

⁹ *Id.*

II. HOMELAND SECURITY DIRECTIVES REQUIRE GREATER PROTECTIONS FOR CRITICAL COMMUNICATIONS INFRASTRUCTURE

Current homeland security directives call on all federal agencies to take appropriate measures to protect critical infrastructure information from casual disclosure. Particularly since the terrorist attacks on September 11, 2001, the federal government has recognized that communications networks are part of the nation's critical infrastructure and vulnerable to harm. In December 2003, the White House issued Homeland Security Presidential Directive 7, which declared that critical infrastructure provide "essential services that underpin American society" and instructed all federal departments and agencies to "identify, prioritize, and coordinate the protection of critical infrastructure ... in order to protect, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them."¹⁰ The current National Security Strategy white paper reiterates the need to enhance domestic security by "protect[ing] and reduc[ing] vulnerabilities in critical infrastructure," including information and communication networks.¹¹ Executive Order No. 12472 calls for the security and preparedness of telecommunications infrastructure in all circumstances, including conditions of crisis or emergency.¹² Presidential Decision Directive/NSC-63 calls on all agencies to protect private telecommunications systems as critical infrastructures, to "focus on preventive measure[s] as well as threat and crisis management," and commit them to "the elimination of our potential

¹⁰ *Critical Infrastructure Identification, Prioritization, and Protection*, HSPD-7, ¶¶ 4, 8 (Dec. 17, 2003).

¹¹ National Security Strategy, May 2010, at 18-19, 27, 31, *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

¹² Executive Order No. 12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions, Apr. 3, 1984 (amended by Executive Order No. 13286 of Feb. 28, 2003 and changes made by Executive Order No. 13407 of June 26, 2006) (the National Communications System "shall seek to ensure that a national telecommunications infrastructure is developed which ... incorporates the necessary combination of hardiness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency."), *available at* http://www.ncs.gov/library/policy_docs/eo_12472.html.

vulnerability [through] a closely coordinated effort of both the government and the private sector.”¹³ President Obama declared December 2010 to be Critical Infrastructure Protection Month.¹⁴

Consistent with this policy, federal agencies have implemented procedures to identify and protect information related to critical communications infrastructure.¹⁵ Congress acknowledged the vulnerability of the nation’s communications infrastructure when it enacted the Homeland Security Act of 2002, which detailed procedures and guidelines for disclosing “sensitive but unclassified information.”¹⁶ The Act exempted information voluntarily shared with the Department of Homeland Security regarding critical infrastructure and protected systems (defined to include communications networks) from FOIA disclosure due to the “actual, potential, or threatened interference with, attack on, compromise of, or incapacitation” of such infrastructure or systems.¹⁷

¹³ Presidential Decision Directive/NSC-63, May 22, 1998, §§ IV, V, *available at* <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

¹⁴ Presidential Proclamation – Critical Infrastructure Protection Month (Nov. 30, 2010), *available at* <http://www.whitehouse.gov/the-press-office/2010/11/30/presidential-proclamation-critical-infrastructure-protection-month>.

¹⁵ *See, e.g.*, Centers for Disease Control and Prevention, *Manual Guide- Information Security*, CDC-02, Exhibit 1 (July 22, 2005) (additional protections for sensitive information regarding communications infrastructure and data networks); 10 C.F.R. § 73.54 (Nuclear Regulatory Commission rule requiring all nuclear power plant licensees to provide “high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks”).

¹⁶ Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (Nov. 25, 2002) (“HSA”) (codified at 6 U.S.C. §§ 131-134). *See also Memorandum for Departments and Agencies*, Laura L.S. Kimberly, Acting Dir., Information Security Oversight Office, Mar. 19, 2002 (establishing the “sensitive but unclassified” category of information and noting that sensitive critical infrastructure information may fall within Exemption 2 of the FOIA), *available at* http://www.dod.gov/pubs/foi/dfoipo/docs/cbrn_wh_memo.pdf.

¹⁷ HSA § 214(a)(1) (codified at 6 U.S.C. § 133)(a)(1). *See also* 6 U.S.C. § 131(6) (defining “protected systems” to include communications networks). It is important to recognize that Internet Service Providers (ISPs) are required to respond to orders issued by the Federal Bureau of Investigation, pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 *et. seq.* Such “Title 50 Orders” require ISPs to facilitate surveillance and the availability of equipment via the headend and general infrastructure of the provider in compliance with the orders. *See generally* 50 U.S.C. §§ 1801, 1802 (a)(1), 1805(a)(3). Wide-scale public availability of geographic vectors that may encompass these security installations could jeopardize national security.

The Commission has committed itself to these national priorities. Last month it committed itself to the very Presidential Directives which call for security of telecommunications infrastructure, preventive measures and the swift elimination of significant vulnerability to critical infrastructures.¹⁸ The White Spaces Order would inadvertently undermine these directives and policies by unnecessarily providing such easy access to sensitive location and critical infrastructure information to potential terrorists and saboteurs.

Given the national interest in reducing risk to critical communications infrastructure, the Commission should adopt reasonable security measures to protect the precise geographic coordinates of cable headends against casual, one-stop browsing, and better protect critical infrastructure for broadband Internet, voice over IP, emergency alert messaging and other critical communications services.¹⁹ Furthermore, such protection will mitigate the risk that cable headend receive antenna specifications in the database (*i.e.* the beamwidth of the antenna and the direction that the main beam is pointed), combined with the exact frequencies used by the antenna, could be used to identify an optimal location to create highly detrimental interference across an entire cable community.

¹⁸ James Arden Barnett, Chief, Public Safety and Homeland Security Bureau, Critical Infrastructure Protection Month (Dec. 21, 2010), available at <http://reboot.fcc.gov/blog?authorId=10511>.

¹⁹ FCC filings made available to the public do not require the coordinates of cable headends. For example, aeronautical filings ask for coordinates of the central point of the system and a radius that encompasses the entire cable plant. A cable operator is required to notify local broadcasters of the location of its principal headend and keep that information in its public file, but that information is not made available to the public in a centralized one-stop online database. Local Exchange Routing Guide (LERG) identifies the connection point used for determining interconnection routes, but this information is not filed at the FCC and is made available only to carriers. The proposed TV band database would be the first comprehensive repository of headend and tower information in a readily-accessible format, available online worldwide on an anonymous basis.

III. SIMPLE ADDITIONAL SECURITY MEASURES CAN PROTECT CRITICAL COMMUNICATIONS INFRASTRUCTURE WHILE MAINTAINING WHITE SPACES FUNCTIONALITY

The Commission should adopt straightforward security requirements that would better protect critical infrastructure by limiting access to such information to such persons that need access to serve the Commission's purposes of detecting errors and facilitating the resolution of interference issues.

Specifically, the Commission should amend Sections 15.711(f), 15.713(a)(1) and 15.713(j) to require that in addition to securing communications between the TV band database and authorized Television Band Devices (TBVDs), each TV band database shall employ adequate security measures, protocols and procedures to restrict all other access, including access for viewing, to registered device manufacturers and operators of broadcasting and communications businesses. As a practical matter, these are the professional entities that would be engaged in resolving interference issues. Additional parties could apply to the Commission for authorization upon a showing that they would use such access for a necessary and appropriate purpose.²⁰

In addition, the Commission should amend Sections 15.711(b)(vi) and 15.711(f) to require that each party that receives TV band database information shall limit use of the information to obtaining lists of channels available for that device to use, and shall employ adequate security measures to ensure that sensitive database information (including the location of communications infrastructure) is secure against accessibility through display, device ports,

²⁰ For example, the Commission could allow database access by a limited number of Commission-vetted white spaces organizations that could provide supplementary review of database information to detect errors – without opening up the database to unlimited access by anonymous, un-vetted parties. All parties permitted to register should be required to be bound by reasonable non-disclosure restrictions to assure that information is not misused or further disseminated.

and unprotected interfaces. This would permit machine-to-machine data flow to operate for its intended purpose, while reducing the risk that sensitive database information will be readily accessible for locating critical communications infrastructure.

These additional requirements would not place an undue burden on any party. The *Order* already requires prospective TV band database administrators to submit their security methods for Commission review. Applications for certification of TV band devices must likewise include a high level operational description of the technologies and measures in place for assuring security.²¹ As with the security procedures already adopted, any reasonable method may be permitted to secure the database against unauthorized access, and the adequacy of such measures can be reviewed by the Commission in connection with the approval of database administrators, in connection with device certification, and from time to time as may be needed for periodic correction.

²¹ 47 C.F.R. §§15.711(b)(vi), 15.711(f), 15.713(a)(1), 15.713(j). The Commission further committed that if such measures proved to be insufficient, it would “take steps to ensure that those measures are quickly corrected by device manufacturers and database administrators or to withhold or withdraw the authorization for operation of any affected devices.” *White Spaces Order* ¶ 100.

CONCLUSION

For the reasons explained above, the Commission should reconsider its decision and adopt the modifications proposed above.

Respectfully submitted,

/s/ Rick Chessen

William A. Check, Ph.D.
Senior Vice President
Science & Technology
Chief Technology Officer

Andy Scott
VP, Engineering
Science & Technology

January 5, 2011

Rick Chessen
Neal M. Goldberg
Loretta P. Polk
National Cable &
Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431