NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

FOR IMMEDIATE RELEASE:
April 21, 2010

NEWS MEDIA CONTACT:
Robert Kenny 202-418-2668
Email: robert.kenny@fcc.gov

FCC LAUNCHES INQUIRY ON PROPOSED CYBER SECURITY CERTIFICATION PROGRAM FOR COMMUNICATIONS SERVICE PROVIDERS

Washington, D.C. – The Federal Communications Commission (FCC) today adopted a Notice of Inquiry (NOI) that seeks public comment on the proposed creation of a new voluntary cyber security certification program that would encourage communications service providers to implement a full range of cyber security best practices. This National broadband Plan recommendation serves as a first step to implementing a comprehensive roadmap to help counter cyber attacks and better protect America's communications infrastructure.

Enhancing the cyber security of the nation's infrastructure is critical to the proper functioning of communications networks serving America's financial institutions, national energy grid, medical institutions, educational system, and public safety. Yet, broadband communications networks are susceptible to malicious attack. Despite the increasing threat of cyber attacks, many communications end-users do not consider cyber security a priority. In 2008, a Data Breach Investigations report concluded that 87-percent of cyber breaches could have been avoided if reasonable security controls had been in place.

The goals of a voluntary cyber security certification program would be to:

- Increase the security of the nation's communications infrastructure;
- Promote a culture of more vigilant cyber security among participants in the market for communications services; and
- Offer consumers (or end-users) more complete information about their communication providers' cyber security practices and ability to better protect their personal computer hardware and online activity from cyber attacks.

The NOI seeks comment on a voluntary certification program under which private sector auditors or the FCC would conduct security assessments of participating communications service providers' networks, including their compliance with stringent cyber security practices developed by a broad-based public-private partnership. Providers whose networks successfully completed this assessment would then be able to market their networks as complying with these FCC network security requirements.

Further, the NOI includes the following questions regarding the proposal:

- The benefits and costs of such a program.
- Whether such a program will create a significant incentive for providers to increase the security of their systems and improve their cyber security practices.
- Whether public knowledge of providers' cyber security practices would contribute to broader implementation by industry.
- Whether the scope of the certification program should be open to all communications service providers or should be limited to certain types of providers. If the latter, how should this be limited?
- What the overall framework should be for the certification criteria.
- The composition of a certification authority and whether it should be open to all segments of the potentially affected industries.
- The operating procedures of a certification authority.
- Who should be responsible for establishing the requirements that auditors must meet to be accredited to conduct cyber security assessments under the proposed program?
- What should be the appropriate certification criteria, accreditation procedures, and requirements to maintain certification once obtained?
- Whether the network security criteria should be definitive and objectively measurable or established on a case-by-case basis.
- The development and application of assessment standards.
- The form and duration of the security certificate, the renewal process, and permissible uses by providers of the security certificate.
- How appeals of certification issues should be handled.
- Whether any Commission enforcement process should be implemented for this program.

The NOI seeks comment on other actions, including voluntary incentives the Commission can take to improve cyber security and asks about actions the Commission can take to better educate consumers, businesses and government agencies about cyber security.

Action by the Commission, April 21, 2010, by Notice of Inquiry (FCC 10-63). Chairman Genachowski, and Commissioners Copps, McDowell, Clyburn and Baker. Separate Statements issued by Chairman Genachowski, and Commissioners Copps, McDowell, Clyburn and Baker. PS Docket No. 10-93.

Public Safety and Homeland Security Bureau (PSHSB) contact is Jeff Goldthorp, Chief of the Communications Systems Analysis Division, at (202) 418-1096.

-FCC-