

I am writing on behalf of (ISC)², a not-for-profit organization dedicated to improving the skills and capabilities of the global information security workforce through professional education and certification and public awareness. (ISC)² has certified over 71,000 information security professionals in 135 countries. We sincerely appreciate your continuing interest in the increasing security of the nation's broadband infrastructure and the promotion of vigilant cyber security public and communications providers.

We also appreciate your continuing interest in the increasing security of the nation's broadband infrastructure and the promotion of vigilant cyber security public and communications providers. A voluntary or mandatory program to develop awareness for both the need to improve cyber security practices and develop approaches to practicably make such improvements is an important public policy goal.

We believe that through a well-crafted public-private partnership such a program can:

- (1) Increase the security of the nation's broadband infrastructure;
- (2) Promote a culture of more vigilant cyber security among participants in the market for communications services; and
- (3) Offer end users more complete information about their communication service providers' cyber security practices.

The creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users and the implementation of their countermeasures in response to cyber threats and attacks is a laudable step in the right direction. The Commission's National Broadband Plan (NBP) recommendation that the FCC should coordinate with the Executive Branch and should also consider including private industry, particularly broadband carriers and information security leaders, to develop the cybersecurity plan. The NBP roadmap was tasked to identify the five most critical cybersecurity threats to the communications infrastructure and its end users and establish a two-year plan, including milestones, for the FCC to address these threats. The NBP stated that "[t]he country needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely."

We understand that developing a strategy to meet the challenges to the nation's infrastructure should be done with the vision of a holistic approach to meet the threat that has become constant and persistent. To that end, we would recommend the following be considered.

1. In the original docket, the concept of certifying broadband carriers was explored. We would encourage the Commission to consider the concept along the lines of following the ISO 27000 certification managed by private entities such as a non-profit organization whose process are ANSI certified. We would support a high level group of security experts to review the industry and develop a list of best practices that are most applicable to broadband service providers based upon threat and risk to the public and the companies.

2. There are a number of published configurations for different platforms and telecommunications parts to the infrastructure that may be used to provide stronger security (http://www.nsa.gov/ia/guidance/security_configuration_guides/ and <http://cisecurity.org/en-us/?route=downloads.benchmarks>). We would recommend reviewing these configuration guides in developing a guideline for the broadband industry providers to assist in develop a risk based approach to the business needs of the broadband carriers.
3. The FCC in addressing vulnerabilities in core Internet protocols and technologies should consider encouraging the move and adoption of more up-to-date technologies such as IPv6 which has more robust security and the encouragement of providing security services and awareness to end users of broadband services. We would advise the Commission and the broadband industry to take an active interest in partnering on the strategy for secure online transactions in developing more secure authentication processes to enable safer business relationships on the Internet.
4. In regards to intrusion prevention and detection, we believe that the Commission should encourage broadband service providers to actively monitor the health of their networks and those of their endusers should an enduser be compromised and endanger the infrastructure and other endusers. We would encourage the industry that when an incident is detected on the infrastructure and deemed to be of sufficient magnitude, it be reported to the proper authorities so that other carriers and the public maybe warned if necessary.

5. In regards to meeting the needs of the country should there be a widespread outage, the Commission should encourage broadband providers to develop plans to manage outages be they a cyber attack or a natural disaster. Currently, the FCC receives outage information but we understand that this is generally a voluntary program that broadband providers and telecommunications companies use. Reporting is to be done on a 12 hour basis by companies that provide outage information. We believe that the Commission should have a more robust reporting or monitoring program to provide a better understanding of the health of the country's telecommunications and broadband carriers so that coordination with the industry can be managed in a timely fashion and notification to other government agency and to the general public should that be necessary. As a final note, the Commission should continue its participation in existing multilateral, regional, and bilateral forums in which cybersecurity is a subject for dialogue, negotiation, or development. In addition, utilizing forums such as the Internet Governance Forum, the Forum for Incident Response and Security Teams (FIRST), and other arenas for dialogue would supplement more formal interactions with established partnerships such as those being driven through the Department of Homeland Security's National Cyber Security Division for government-to-government collaboration and cooperation.