Testimony of
James Arden "Jamie" Barnett, Jr.
Rear Admiral, USN (Retired)
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission
Senate Committee on Commerce, Science and Transportation
Hearing on "Cybersecurity: Next Steps to Protect Our Critical Infrastructure"

February 23, 2010

Senator Rockefeller, Ranking Member Hutchinson and distinguished Members of the Committee, thank you for the opportunity to testify on the important topic of cyber security, and thank you for your leadership in holding this hearing to address this urgent problem.

My remarks to you today are focused on the transformation of communications by the Internet and broadband technologies, the cyber threat that transformation has engendered, and how the traditional role of the Federal Communications Commission to ensure communications is being invigorated to meet the challenge of the cyber threat.

Advanced broadband communications technologies have dramatically changed the lives of Americans and others around the globe by enriching the way they communicate, learn, work and live. The Internet, which relies on broadband communications infrastructure, is now a central part of American interaction of all types. However, the manner in which the Internet developed has left it exposed to cyber attacks. Specifically, the Internet, which started as a small research network, has evolved into a global network connecting over a billion people who rely on it for social, economic, educational and political applications, among others. The Internet's core design philosophy was initially based on easy connectivity. The underlying Internet protocols and architecture were not designed to be secure. As Internet usage has increased and has

become mainstreamed for everyday life, communications providers have responded by adding features to improve the security of their infrastructure and the services that ride on it.

As the public and private sectors continue to move towards more online usage, bad actors, including criminals, have begun to lurk in the shadows of cyberspace where they can launch costly attacks on end-users. In 2008, the FBI Internet Crime Complaint Center logged $265 million in reported losses for Internet users, the highest loss ever reported. No one is immune from attack, whether consumers, government users or even our nation's most sophisticated companies. Last year, it was reported that ten to twenty terabytes of data were pilfered from U.S. government networks by a foreign entity, and in January Google reported that it was subject to a sophisticated attack originating from China. Reports show that at least ten other large companies, including finance, media and chemical companies, have been the targets of similar attacks. As attacks become more persistent, breaching computer systems and establishing a foothold, these attackers are able to compromise personal, confidential and classified information. We have seen the effects of dedicated cyber attacks on Estonia and the Republic of Georgia. Critical infrastructure sectors, such as energy, finance and transportation, can all fall victim to these attacks.

All major communications networks are now connected to the Internet, and for that reason, those communications networks are vulnerable to cyber attacks. Most cyber attacks target information systems attached to communications networks, the edge or end-users, not the communications infrastructure itself. Cyber attackers currently tend to

view the communications infrastructure as the necessary superhighway that will carry them to their victim. Accordingly, they are reluctant to make it impassable.

Nonetheless, communications infrastructures are not immune to cyber attacks, and they have known vulnerabilities. Accordingly, we should not have a false sense of satisfaction with regard to the survivability of our broadband infrastructure. A successful attack on communications networks can affect all end-users that rely on broadband infrastructure. For example, as 9-1-1 networks migrate from today's technologies to Internet-based technologies concerns about the vulnerability of these systems to cyber attacks have mounted. A successful attack on such a network could severely obstruct the ability of our first responders even knowing of emergencies.

We cannot allow the absence of a successful attack make us complacent. The FCC has an important role to play in securing broadband communications infrastructures. We are the Congressionally-mandated regulatory agency with authority over communications providers and communications networks. We must face the new reality that cyber threat now imperils our communications networks and therefore our well-being and even lives.

With the changing shape of the telecommunications infrastructure and usage patterns, it is incumbent on the FCC to reassess our role in cyber security. When I came aboard as Chief of the Public Safety and Homeland Security Bureau, FCC Chairman Genachowski asked me to convene a ninety-day working group to examine the Commission's cyber security posture and recommend future courses of action. This group delivered its report to the Chairman on November 30, 2009 and many of its recommendations will be addressed in the National Broadband Plan that will be

submitted to Congress in March. Our Working Group report demonstrates the critical role that the FCC has in cyber security, in conjunction with its federal partners. This report, in conjunction with the National Broadband Plan, leads us to our plan to become further engaged in cyber security. To this end, we have developed a roadmap in which we plan to address cyber security utilizing our past experience, technical expertise and our regulatory relationship with the FCC's licensees to protect the communications infrastructure. I would like to mention six major points from that roadmap.

First, we believe, based on past experience, that many cyber security challenges can be met through public-private partnership arrangements with industry. However, it would be ill-advised to assume that intervention is not needed. In some cases, obligations may be necessary. The Commission has a vital role to play in these situations, and we will be working to craft a regulatory approach to cyber security that strikes the right balance.

Second, we believe there are things the FCC can do to prevent or mitigate the effects of cyber attacks. For example, recently, the Network Reliability and Interoperability Council, an FCC federal advisory committee consisting of leading industry executives and practioners, developed a set of detailed cyber security best practices that are intended to be implemented by communications providers on a voluntary basis.

We believe the opportunity exists for us to build on these best practices to provide network operators additional ability to improve their cyber security and to increase the adoption of these best practices. A recent survey by PricewaterhouseCoopers found that organizations following best practices experienced significantly lower impact from cyber

attacks, something that commercial industry should find attractive. We believe that based on this survey that we should explore methods, such as voluntary certification of compliance with best practices that would create market-based incentives to increase cyber security.

Third, we believe that a significant area for FCC involvement in cyber security is to secure and analyze additional data received from all broadband service providers concerning network and service disruptions. However, our past experience in receiving data from communications providers concerning disruptions in their networks has been proven effective at providing us early warning of potential problems and attacks on the Nation's existing communications infrastructure. This information allows us, working with our Federal partners and the communications industry, to expedite restoration of service. Our work, which is based on a sector-wide view of communications outages, also allows us to spot industry-wide or carrier-specific reliability and security matters. We use this information in conjunction with DHS and communications providers to produce long-term improvements. For example, we recently observed a statistically significant upward trend in the number of events affecting wireline carriers. We worked with industry to establish a team of experts who examined the data in closer detail and developed a set of recommendations. In the intervening months we have measured a 28% decline in this category of outages. Obtaining similar information from broadband and Internet service providers would enable the FCC and its federal partners to work with industry on sustained improvements to Internet-based infrastructure. We are currently examining the best path forward to obtain this information.

A fourth way in which we are exploring more active involvement in cyber security is increase our ability to prepare reports which contains situational awareness on broadband communications infrastructure during disasters for use by our federal partners, such as the Department of Homeland Security (DHS). We currently gather such data for traditional communications, and it has proven invaluable in emergency management and communications restoration. Accordingly, we plan to coordinate with DHS and communications providers in the near future to plan and implement a cyber attack situational awareness system.

Fifth, another avenue we are pursuing is how to best address the constant steam of malware arriving at the network, frequently from end-users who are not aware that their systems are compromised. The Commission has recently established an advisory committee, the Communications Security, Reliability and Interoperability Council, known as CSRIC. An important function of the Council is to examine this problem and to recommend methods that communications providers can implement to protect their networks from malicious traffic. We expect to see reports from this Council in the near-term.

Sixth, and finally, cyber security is by nature international. The networks are global, the threats are worldwide, and the human component is universal. Through the State Department, the Commission participates in various international activities and fora such as the United Nations International Telecommunication Union (ITU) in which cyber security is an issue. Cyber security is increasingly raised as an issue in discussions with foreign regulators and at international meetings and conferences, and the international aspects of

cyber security is also a more prevalent topic in the domestic arena. Going forward, there will be increased need and opportunities for, greater FCC participation in activities involving international aspects of cyber security – both in the United States and abroad.

My intention has been to describe to you our vision of the FCC's role in cyberspace and what we are doing to secure our critical communications infrastructure in a broadband world. We are at the start of a long journey, working with our Federal partners and industry, to secure our Nation's vital infrastructure against a new and rapidly evolving threat, and we are determined to do so.

Thank you for the opportunity to speak to you today.