House Permanent Select Committee on Intelligence

Statement of John C. Nagengast
Member, CSIS Commission on Cyber Security for the 44th Presidency

18 September 2008

Thank you, Mr. Chairman and members of the Committee for the opportunity to testify before you today. It is an honor to offer my perspective on the implications of the CSIS Cyber Security Commission's emerging recommendations on the Intelligence Community. I believe the recommendations are both comprehensive and compelling, and provide a significant basis for action by the next President and the Congress in addressing this important issue.

Need for a Comprehensive Cyber Strategy, Leadership, and Collaboration

First and foremost, the Commission report points out that the U.S. lacks a comprehensive cyber space strategy, nor is anyone actually in charge of developing such a strategy or assuring the defense of our national interests in cyber space. Creating a position within the Executive Office of the President (EoP) to deal with these issues is an obvious first step to filling this void. Given strong leadership from the EoP, it is imperative that the Director of National Intelligence (DNI) and key cyber space players within the Intelligence Community are closely linked to, and highly supportive of, the development and execution of the strategy. The DNI and the Intelligence Community must break new ground in bringing their skills and capabilities to the fight. The private sector must be engaged in new ways to defend our critical cyber systems, as well as to maintain the technology leadership in cyber technology which the United States has enjoyed in the past, but has now eroded significantly.

CNCI and the Need for a More Open, Inclusive Dialog

I would also note that the Comprehensive National Cyber Initiative (CNCI) has made a good start in bringing attention to the cyber security issue, and putting some basic capabilities in place to better defend government information systems. The CNCI has, in fact, become the de facto national cyber strategy. I also applaud the recent efforts to make some of the aspects of the CNCI more visible - but these are only first steps. I certainly recognize the need for secrecy in some of the aspects of the CNCI, but an effective national strategy must certainly be openly vetted and publicly debated in order to be credible and widely accepted. The DNI and the members of the Intelligence Community must support that debate by removing the shroud of secrecy around the CNCI, and by serious engagement with

the various private sector stakeholders in cyber technology and security. This would lay a solid foundation for the next Administration to build upon.

Framework Needed to Facilitate Cooperation, Safeguard Privacy

I would also point out that the necessary increase in cooperation between the government and the private sector in defending cyber space will require the creation of a new policy and legal framework to assure that relevant cyber information can be exchanged and mitigation activities taken in a timely manor, while assuring that privacy is maintained and the equities of private sector participants protected. This policy and legal framework must be consistent with and supportive of comprehensive strategy for cyber space which I mentioned earlier. With the exception of the recently-enacted FISA Modernization Act, most of the legal framework which now governs identification and mitigation of malicious activity in cyber space was created many years ago around circuit switched telephone communications, and is hardly relevant or effective today. Creation of a new policy and legal framework to enable effective defense with expanded cooperation between the government and private sector will be a monumental undertaking, with broad implications nationally and internationally. The DNI and the members of the Intelligence Community must rise to the occasion in providing positive support to this effort, working proactively with the Congress to provide an effective and relevant legal framework for cyber security the 21st century. The DNI must assure that all of our national security interests are represented in creating a comprehensive policy and legal framework for the full range of cyber space operations in the future, for the U.S as well as our allies and intelligence partners.

Successful Partnership will Provide Value to All Parties

In closing, it is critical that the DNI and the Intelligence Community immediately demonstrate that they can provide real value in partnering with the key private sector stakeholders to defend critical information systems. It is fair to describe most of the existing partnership efforts to date as less-than-successful, and many in the private sector view them as unproductive. Future discussions of partnership and expanded cooperation are meaningless unless there is obvious benefit to participation in the partnership. A streamlined and effective process for sharing relevant information is essential to expanding security in cyber space. The DNI and the Intelligence Community must demonstrate they can provide useful, actionable cyber information in timely fashion.

Thank you again for giving me the opportunity to speak to you today. I look forward to answering your questions.