Senate Homeland Security and Government Affairs Committee

Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century

Statement for the Record

Frances Fragos Townsend
Chairwoman of the Board
Intelligence and National Security Alliance

June 15, 2010

Chairman Lieberman, Ranking Member Collins, Senator Carper and members of the Committee, thank you for the invitation to testify at this hearing and to offer my thoughts on the *Protecting Cyberspace as a National Asset Act of 2010*. I am here today in my role as the Chairwoman of the Board of the Intelligence and National Security Alliance (INSA). INSA is the premier not-for-profit private sector professional organization providing a structure and interactive forum for thought leadership, the sharing of ideas, and networking within the intelligence and national security communities. INSA has over 100 corporate members, as well as several hundred individual members who are leaders within the government, private sector and academia.

Through its Cyber Security Council, INSA has emphasized the importance of creating a strong public-private partnership that can provide meaningful recommendations to address this national and economic security threat. Today I would like to specifically speak to the importance of establishing a public-private partnership to promote national cyber security priorities, strengthen and clarify authorities regarding the protection of federal civilian systems, and improve national cyber security defenses.

Collective national cyber security can only be effectively addressed through a partnership approach between government and private industry. While the government has the legal and moral authority required to organize markets, enforce laws and protect citizens' privacy and property, the vast majority of cyberspace infrastructure is privately owned and operated. As a result, industry is where most of the expertise in the fields of IT and cyber security reside. The private sector cannot protect privacy and address security while the government cannot dictate security regulations to networks systems it cannot control. Furthermore, attempts to do so could stifle innovation and profitability. Because of this dynamic, partnership is the only way forward.

INSA's Cyber Security Council studied several different models of public-private partnerships during the preparation and research for its November 2009 report, *Addressing Cyber Security Through Public-Private Partnership.* Historically, effective public-private partnerships have inclusive private sector membership, unified in the pursuit of common goals, a single responsible and accountable government partner organization and clearly delineated roles for both public and private entities. We are very pleased to see these concerns and this organizational structure reflected in the legislation we are discussing today. This bill not only establishes a clearly responsible Center for the problem, but requires that a private sector advisory council be organized to advise the Center on their actions' effects on industry.

Assuring that private sector concerns are heard within government is an important first step to the creation of a public-private partnership, but this alone is not sufficient to guarantee success. INSA's Cyber Security Council has identified three key additional components, specific to a public-private partnership on cyber security, which would be required for a successful effort: a flexible or incentivized approach to regulation, robust information sharing and cooperation and communication on standards and best practices.

With regards to flexible and/or incentivized regulation, it is crucial that government, to the best of its ability, preserve and nurture the innovative and entrepreneurial environment that exists in information technology. A free flow of information and the use of an open source environment has created capabilities and driven the development of new business. Prescriptive or directive security standards, or one-size fits all approaches will limit innovation and erode industry support and participation if industry managers feel security mandates have made their business less competitive. Securing networks and the cyber environment while allowing businesses to remain dynamic in that space is a difficult needle to thread and we applaud the measured approach of this bill in allowing industry members to propose their own security solutions for approval by the regulatory body. This not only creates a true give-and-take security partnership, but also allows for innovation and growth with the development of new procedures and products.

Also critical to a strong public-private partnership is the creation of a shared awareness of the network environment. Information sharing is absolutely crucial and is an area in which we are presently falling short. Classification, concerns over liability and the present situation in which cyber security is not "owned" by anyone all contribute to this shortcoming and there are sections of this bill that do help. The liability protections afforded to those in compliance with government security measures do provide protection and incentive to private sector firms to increase their reporting, but until the private sector feels they are getting as much as they are giving with respect to information sharing and incident reporting, the system will remain insufficient. The bill calls for the establishment of plans for information sharing between public and private entities and industry should certainly watch this process closely and press for a commitment from the executive branch to share information with the private sector that is as strong as the private sector's responsibility to report to the government.

The final component, cooperation in the development of standards and best practices, is perhaps the most crucial. Government must develop security standards and systems that deal with known threats and have the capacity to adapt to the rapidly changing cyber environment, and it must do so in concert with industry partners. Just as directive regulations can limit innovation, security standards that are not developed in partnership with businesses

can have adverse and unplanned consequences. The vetting of proposed security standards through the industry community is necessary to avoid undue burden and hardship for American business. But the private sector cannot carry out this process entirely on its own; they need strategic-level threat information and cross-sectional situational awareness from the government to create standards which address actual threats and vulnerabilities and make the nation safer. In this bill, the new Center for Cyber security and Communications assesses and evaluates cyber security standards and guidelines, and makes recommendations recognizing existing NIST and industry standards, an important step toward joint production of security protocols. The second step must be carried out by the Center itself when creating its standards and bringing them to industry. They should embrace a true partnership approach, soliciting comments from industry on draft proposals, consulting closely with owners and operators and being open to revision of their rules in light of industry input.

The INSA Cyber Security Council recognizes that there are a number of ways to address cyber security and believes the effort to do so should begin right away on three fronts: private sector self-regulation, executive branch leadership and congressional action. Self regulation is not an unprecedented activity in the U.S private sector. There are multiple examples of where the private sector has self-organized to attain a goal. Examples are the North America Electric Reliability Corporation, volunteer Fire Departments, school boards, community associations, etc. Self regulation in cyber space can be achieved and self imposed based on a strong value proposition and value-based incentives. However, only the government, contained by law, can fully investigate the behavior of individuals or groups, apprehend, prosecute and punish those who violate the law or defend against and respond to threats and attacks against the nation's interests. Hence a government role, within DHS like the one identified in the bill, is absolutely essential.

Finally, the role of Congress to enhance the security and resiliency of the cyber and communications infrastructure of the United States is critical to make well-informed decisions and respond to problems quickly. Congressional oversight is also important to ensure that the goals and objectives of the National Strategy are being met, particularly as they relate to use of legal authorities for cyber missions and the reasonable privacy expectations of U.S. persons.

With this bill, the Senate has taken the lead in identifying cyber security needs and organizing the government to address them. This measure relies on the executive branch for the establishment, implementation and development of new structures, protocols, plans and oversight. This Committee, as well as the private sector will have to engage with the executive branch and monitor the implementation of the provisions of this bill to ensure that this new organizational structure reflects the spirit of the law and does not place undue or unanticipated

counterproductive burdens on both government agencies and private sector companies. The goal is to make a positive and meaningful contribution to the national security of the United States and this bill goes a long way towards achieving that goal.