US House of Representatives
Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection, and Cyber Security

Testimony of Paul B. Kurtz
Executive Director
Cyber Security Industry Alliance

April 20, 2005

Thank you, Chairman Lungren and Ranking Member Sanchez for inviting the Cyber Security Industry Alliance (CSIA) to testify before this subcommittee in reference to HR 285. I would also like to acknowledge Congressman Thornberry and Congresswoman Lofgren for their continued efforts in support of an Assistant Secretary for Cyber Security position in DHS. Their bi-partisan work is evident in their co-sponsorship of this bill.

As Executive Director of CSIA, I am pleased to speak about the need for an Assistant Secretary for Cyber Security in the Department of Homeland Security. CSIA supports rapid passage of HR 285.

The members of the Business Software Alliance also support this legislation and I am also speaking on their behalf.

Since the late 1990s, we have spoken of a "partnership" to secure the critical infrastructure of the United States, particularly the information infrastructure, since it is owned and operated by the private sector. For this partnership to truly be successful and not simply rhetoric, we need a clear leader in the Department of Homeland Security to act as a focal point for this partnership. A Director-level position does not have the sufficient stature or programmatic authority for accountability, or to reach across sectors. A leader in securing the critical infrastructure must have the authority and resources to accomplish this important and complex mission.

This leader must be at least at the Assistant Secretary level to have the impact that is needed.

Unlike other sectors, the information infrastructure is dynamic and will continue to evolve for the foreseeable future. Changes within the information infrastructure are driving change in all other sectors. Cyber and physical infrastructure security will receive greater respective attention with an Assistant Secretary for Cyber Security working alongside the Assistant Secretary for Infrastructure Protection, while remaining integrated under the leadership of the Undersecretary for Infrastructure Protection and Information Analysis. It is particularly important that the Assistant Secretary for Cyber Security have primary authority over the National Communications System, given the convergence of voice and data networks.

CSIA strongly believes that the Federal government needs a comprehensive approach to cyber security protection. The establishment of an Assistant Secretary for Cyber Security in the Department of Homeland Security is a critical initial step in this approach.

I will cover three areas in my testimony:

- A brief introduction to CSIA

- An overview of the roles and responsibilities of the Department of Homeland Security in the area of cyber security
- The importance of clear leadership on the issue of cyber security

Introduction to CSIA

CSIA is dedicated to enhancing cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. CSIA is the only CEO-led public policy and advocacy group exclusively focused on cyber security policy issues. We believe that ensuring the security, integrity and availability of global information systems is fundamental to economic and national security. We are committed to working with the public sector to research, create and implement effective agendas related to national and international compliance, privacy, cybercrime, and economic and national security. We work closely with other associations representing vendors as well as critical infrastructure owners and operators, as well as consumers.

Members of the CSIA include BindView Corp; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc.; iPass Inc.; Juniper Networks, Inc.; McAfee, Inc; PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation; Symantec Corporation and TechGuard Security, LLC.

CSIA understands that the private sector bears a significant burden for improving cyber security. CSIA embraces the concept of sharing that responsibility between information technology suppliers and operators to improve cyber security. Cyber security also requires non-partisan government leadership. Work to strengthen cyber security began in the Clinton administration. The Bush administration has continued and boosted this work, through the creation of the National Strategy to Secure Cyberspace. The National Strategy remains timely and salient.

Roles and Responsibilities

Last December, the Cyber Security Industry Alliance released an agenda for the administration that outlined twelve steps to help build a more secure critical infrastructure that called for an Assistant Secretary level post in the Department of Homeland Security. To understand why we feel this is critically important to the protection of our cyber infrastructure, I thought it would be helpful to expand on the Agenda and offer a framework to help define Federal versus private sector responsibilities in the area of cyber security.

By outlining the responsibilities of the Department of Homeland Security in the area of cyber security, we feel that the need for an Assistant Secretary-level position can be better understood.

Three Federal documents provide a framework for Federal responsibilities to secure cyberspace:

- The President's National Strategy to Secure Cyberspace (February 14, 2003)
- Homeland Security Presidential Directive-7 (December 17, 2003)

- The National Response Plan's Cyber Incident Annex (January 6, 2005)

President's National Strategy to Secure Cyberspace

The President's National Strategy is an appropriate place to start. While the Strategy's recommendations receive substantial attention, it also provides clear policy guidance on the Federal government's role. The President's cover letter for the Strategy states:

"The policy of the United States is to protect against the *debilitating disruption* of the operation of information systems for critical infrastructures and, thereby help to protect the people, economy, and national security of the United States." He continues, "We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our nation's *critical infrastructure* and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable and cause the least damage possible."

The strategy adds some additional guidance on its role, noting that it is appropriate for the government to assist with forensics, attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against *organized attacks* capable of inflicting *debilitating* damage to the economy.

Additionally, Federal activities should also support research and development that will enable the private sector to better secure privately-owned portions of the nation's critical infrastructure.

These statements lead to the conclusion that Federal activity is bounded to protecting against ***debilitating*** attacks against ***critical infrastructure***, attack attribution for national security systems, forensics and research and development.

The Strategy also sets specific responsibilities for Federal agencies, including the Department of Homeland Security. The Strategy states that the Department should:

- Develop a comprehensive plan to secure critical infrastructure.
- Provide crisis management and technical assistance to the private sector with respect to recovery plans for failures of critical information systems
- Coordinate with other Federal agencies to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local and nongovernmental organizations including the private sector, academia and the public
- Perform and fund research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

It is important to note that the Strategy does not place responsibility for every problem associated with cyber security with DHS, but focuses its role on contingency planning and emergency communications – two critical areas of defense against threats to our national security.

HSPD–7

HSPD-7 establishes the U.S. government's policy for the identification and protection of critical infrastructure from *terrorist* attacks. It advances the President's strategy in a number of areas and helps further refine the Federal government's role in securing cyberspace.

HSPD-7 focuses in large part on the identification and protection of assets that if attacked would cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction. It also addresses the protection of infrastructure that if attacked would:

- Undermine state and local government capacities to maintain order and to deliver minimum essential public services.
- Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services
- Have a negative effect of the economy through the cascading disruption of other critical infrastructure and key resources.
- Undermine the public's morale and confidence in our national economic and political institutions.

HSPD-7 designated the Department of Homeland Security as a focal point for information infrastructure protection, including cyber security, stating:

"The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems."

The National Response Plan's Cyber Incident Annex

The National Response Plan (NRP) upholds the President's National Strategy to Secure Cyberspace and HSPD-7. The NRP Cyber Incident Annex states that the Federal government plays a significant role in managing intergovernmental (Federal, state, local and tribal) and, where appropriate, public-private coordination in response to cyber incidents of *national significance.*

A Framework for Federal Action

The President's National Strategy to Secure Cyberspace, Presidential Directive 7 and the National Response Plan yield a possible two-tier framework for Federal responsibility.

Tier One – Functions Critical to U.S. Economic and National Security

1. Identify and prioritize critical information infrastructure that if disrupted would have a debilitating impact on critical infrastructure or systems essential to U.S. economic or national security
2. Prepare for such contingencies by ensuring survivable communications networks among key critical information infrastructure operations in the government and private sector
3. Prepare contingency plans in the event of a disruption that include crisis management and restoration of critical networks, and regularly exercise, test and refine these plans.
4. Provide warning of attack or disruption to critical infrastructure owners and operators from resources or capabilities that are *not* available to the private sector through such means as intelligence.

Tier Two – Supporting Functions that Improve Coordination, Awareness, Education and Personnel Readiness

1. Facilitate coordination between individual sectors of the economy by establishing appropriate government advisory committees
2. Facilitate and support general awareness among all information system users, including home users and small businesses
3. Track trends and costs associated with information infrastructure attacks and disruptions, through such means as U.S. CERT.
4. Coordinate and support long-term research and development for cyber security.

The Importance of Clear Leadership on the Issue of Cyber Security

When you look closely at the responsibilities of The Department of Homeland Security in the area of cyber security, you see that while it may be narrowly defined, its responsibilities are extremely significant to our economic and national security. ***DHS is the government's focal point for the prevention, response and recovery from cyber security incidents that have a debilitating impact on our national and economic security.*** While the private sector has a critical role to play in the protection of critical information infrastructure, DHS serves as the government's and nation's point of coordination for all our efforts. Senior DHS leadership is needed to build an effective government-private sector relationship, to understand the technical and global complexities of cyber security, and to marshal the resources necessary to provide an effective partnership with private sector organizations and initiatives.

Cyber vs. Physical Infrastructure Protection

By advocating for an Assistant Secretary for Cyber Security, we are not dismissing the need to integrate cyber and physical infrastructure protection. Nor are we saying that the protection of the cyber infrastructure is more important than the protection of the physical infrastructure – although it is increasingly a critical component in the operation of our physical infrastructures, and in fact, it cuts across all of our physically infrastructures. The physical and cyber infrastructures are related, but they are fundamentally different in a variety of ways. For example:

- Cyber infrastructure is attacked and defended differently than the physical infrastructure. Cyber infrastructure is largely defended by technical specialists, not through guns, gates, guards, and cameras. Vulnerabilities are discovered through technical means and often require immediate remediation involving a variety of parties across different sectors of the economy. A cyber attack may be launched remotely, requiring no physical access to a target. Cyber attacks may not necessarily be abrupt. For example, a cyber attack may be "low and slow," changing or otherwise corrupting critical data over an extended period of time.

- Cyber infrastructure is dynamic, where the physical infrastructure is more static. For example, power plants, power lines, chemical plants, railroads, bridges remain stationary with more gradual changes in technology, where information networks are rapidly changing. An IP-based transaction may traverse the globe via satellite, wireless, or terrestrial cable. The technologies that support these different means are changing rapidly.

In an event of national significance affecting one or more of the physical infrastructures, the cyber infrastructure takes on additional responsibility for ensuring we have the ability to coordinate and respond to attacks. Our IT infrastructure is operational; without it, our national response capability is crippled.

We believe it is appropriate to have an Assistant Secretary for Cyber Security working along side an assistant secretary responsible for securing the physical infrastructure under the leadership of an Under Secretary as proposed in H. 285.

Conclusion

Mr. Chairman, we are seeing increased threats and vulnerabilities associated with our information infrastructure. We rely upon our information infrastructure, yet there is no one clearly in charge of coordinating its security and reliability. Presidential guidance and the Homeland Security Act clearly identify the Department of Homeland Security as the most appropriate focal point for coordinating the protection of our information infrastructure. We strongly support HR 285 and its creation of a more senior position at DHS to lead efforts to build a more secure information infrastructure for both the government and private sector.