Testimony of Paul B. Kurtz
Executive Director, Cyber Security Industry Alliance
Before the House Armed Services Committee
October, 27, 2005

Thank you Chairman Akin and Cooper for the opportunity to testify before the House Armed Services Committee, Panel on Asymmetric and Unconventional Threats.

The Cyber Security Industry Alliance (CSIA) is the only global public policy organization focused exclusively on information assurance. CSIA is a CEO-led organization that brings together the leaders in information security technology with policy expertise on critical information assurance public policy issues, such as the protection of personal information, spyware, and information infrastructure resiliency.

While in government, I served at the White House on the National Security Council and Homeland Security Council. On the NSC, I served as Director of Counterterrorism and Senior Director of the Office of Cyberspace Security. On the HSC, I was Special Assistant to the President and Senior Director for Critical Infrastructure Protection.

I am pleased to speak on the topic of information assurance and superiority.

The Department of Defense faces several serious challenges with regard to information assurance and information superiority. Critical issues requiring attention include:

- Securing war fighting and defense capabilities and operations that depend on privately owned and operated information infrastructure and hardware and software produced around the globe.
- The need to build and support an information infrastructure that is resilient and can operate under duress or attack.
- DOD’s role to protect, defend and respond to a cyber incident of “national significance” which does *not* involve assets critical to its operations or under its immediate control.

- The absence of a national policy to *assure* the security of critical U.S. information technology and telecommunications infrastructures.

Resolution of each of these issues will have a dramatic impact on DoD's resources and force structure.
Cyberspace is a tough neighborhood, full of accidents, glitches, and attacks. Significant disruptions occur every day. For example, a major backbone provider last weekend suffered a complete outage caused by an error in router configuration. While this was not an attack, restoration of the system required "powering down" routers and bringing them back on line slowly. The speed of attacks is accelerating and becoming more sophisticated: in 1999 the Melissa virus took three days to cross the Internet, in 2001 Code Red took minutes. We are facing the prospect of "zero" day attacks, giving operators little or no time to react. As a reminder, the 2003 Northeast blackout spread within 43 seconds. This brings new significance to the "bolt from the blue."

We must plan for the unexpected and think the unthinkable. Just because a massive attack has not happened doesn't mean it will not occur. We also must think about insidious attacks. For example, the manipulation or corruption of data involving the alteration of target sets or soldiers' blood types, or scrambled logistics orders sending supplies to the wrong places before a critical deployment. The results could be catastrophic and difficult to untangle.

To add to the mix, technology is changing rapidly, including the convergence of the public service telephone network with IP-based networks, the deployment of new technologies ranging from Radio Frequency Identification tags to nanotechnology.

Finally, nation states are beginning to understand the critical importance of the information infrastructure – witness the current firestorm over the prospect of the UN "governing" the operation of the Internet's Domain Name System. Politics is beginning to enter the operation and control of the Internet.

Dependence on Privately Owned and Operated Critical Infrastructure

DoD is largely dependent on an information infrastructure that is owned and operated by the private sector. For example, DoD shares the information infrastructure backbone with the private sector, which means the same attacks which disrupt private sector networks can affect DoD systems. Further, the vast majority of IT products it uses are manufactured by vendors with facilities and personnel from around the world. Ownership of key suppliers is not static. Recently, several telecommunications networks have changed hands, including to entities of potential concern to the Defense community.

It is not practical, efficient, or possible to build an air gapped “parallel universe” of information infrastructure to support Defense operations. DoD must connect with other agencies in the Federal government, allies, and the private sector in order to operate. Given the global economy, it is not easy or advisable to “block” the sale of certain assets to foreign parties. Finally, software and hardware can be subverted by insiders, making even draconian procurement policies of limited value.

This situation poses a vexing challenge that requires consistent, high level attention. Rigor in the procurement process and a comprehensive information assurance program will increase the information assurance. This requires escalating the importance of information assurance within the Defense. Such a program must involve the triad of people, process, and technology. DoD must secure the operation of traditional weapon systems, but they must also secure logistics supply, health, and finance.

DoD should continue to expand the use of security technologies, taking care to use multi-factor authentication, strong access controls, and encryption. DoD should take particular care to address the insider threat. DoD dedicated significant resources into securing the perimeter of classified and unclassified systems. Several organizations within DoD constantly monitor and improve outwardly facing systems for perimeter defense. However, it appears that less energy has been focused on securing information behind the perimeter.

However, simply locking down DoD’s own systems is not enough. DoD must more aggressively reach out to the private sector to identify critical dependencies and work in partnership with the private sector to ensure critical supporting infrastructures are secure and reliable. Such outreach could utilize the National Guard. For example, members of the National Guard who work in information technology could be trained and used to support the defense of DoD networks during normal operations, but also during a crisis. Such training would also be of benefit to the private sector which operate infrastructure of critical value to DoD.

Building and Supporting Resilient Networks

The Defense Department must expect some attacks to succeed. Therefore, the Defense's information infrastructure must be resilient and able to degrade gracefully. This requires a multi-pronged effort which requires supporting efforts to secure infrastructure beyond DoD's immediate control. For example, little attention has been given to securing the basic protocols the support the Internet. An attack against an obscure but important protocol could cause wide-spread disruption. DoD should also rapidly adopt the more secure IPv6 and DNSSEC on all .mil zones.

The vast majority of work in this area rests on research and development. Unfortunately, cyber security has been left by the wayside in terms of Federal funding for R&D and much of DoD's work in information security remains classified. For example:

- **Defense Advanced Research Projects Agency**. The FY 2005 budget for cyber security R&D is $50 to $100 million, but almost all of that is classified.
- **Advanced Research and Development Agency**. The FY 2005 budget of $17 million for cyber security R&D focuses entirely on the intelligence community.

Certainly some work must remain classified. However, a secure and reliable DoD network sitting on top of an inherently vulnerable infrastructure will do little good. DoD should invest money in partnership with DHS and the National Science foundation to develop new secure networks which will replace today's Internet. CSIA has published a white paper noting several areas requiring research which draws upon the excellent work of the President's Information Technology Advisory Committee (PITAC) which was released earlier this year. The PITAC report calls out ten areas requiring additional research, including authentication, monitoring, securing fundament protocols, holistic system security, mitigation and recovery, and cyber forensics. I am joined by Dr. Eugene Spafford, formerly a member of the President's Information Technology Advisory Committee (PITAC), who can speak in detail regarding the Committee's findings.

DOD's Role in an Incident of National Significance

DoD's role is unclear during a cyber incident of "national significance" which does *not* involve assets critical to its operations or under its immediate control. This also raises the issues of DoD's almost exclusive focus on protecting and defending its own systems with little attention to the private sector.

With regard to the latter, currently DoD's indications and warning appears almost exclusively focused on securing its own assets. While this is understandable, it is potentially a grave mistake, particularly given that privately operated information infrastructure may be the *real* target of a terrorist or nation state attack as opposed to DoD's. DoD must expand its indications and warning program to include information on potential action against key elements of the private sector, including banking and finance, transportation, energy, and health care. DoD's efforts must be fully integrated into a National Cyber Attack Sensing, Warning, and Response Capability.

This issue leads to DoD's role in *responding* to an incident of national significance. The Department of Homeland Security (DHS) is responsible for coordinating the response to such an event. However, in the wake of Hurricane Katrina, it is reasonable to question whether this is advisable or practical. During Katrina, local, state, and Federal civilian forces were *overwhelmed.* DOD stepped in to coordinate and respond and to bring order out of chaos. A similar scenario could occur in the case of a massive cyber attack or disruption. Federal civil capabilities could quickly be overwhelmed, and DoD will be called upon to take a leading role. Clearer lines of authority must be drawn to ensure the Federal government can effectively respond to such an incident. In this case, joint exercises involving DHS and DoD, as well as key players in the private sector, should be held to "test" capabilities and coordination. DoD should be requested to develop such contingency plans.

Absence of a National Information Assurance Policy

Currently, there is no Presidential directive that sets national policy and procedures to assure the security of critical U.S. information technology and telecommunications infrastructures. The complex and dynamic nature of information security requires focused leadership within government, along with a close and meaningful partnership with the private sector. Such a directive would address many of the issues outlined in this testimony, including the dependency of DoD’s infrastructure on civilian controlled assets, resiliency, early warning, and clear lines of command and control in case of an incident of national significance.

Such a directive is needed not only to establish a national policy, but to better organize the roles and responsibilities of all the government-related entities’ players involved in information security. Currently, at least eight agencies and organizations address pieces of the problem. Several have overlapping responsibilities and membership. In addition, seven committees and commissions are active, including the President’s Homeland Security Advisory Council (PHSAC), the former President’s Information Technology Advisory Committee (PITAC), the National Security Telecommunications Advisory Council (NSTAC), the National Infrastructure Advisory Council (NIAC), the FCC’s National Reliability and Interoperability Council (NRIC), the Committee on Foreign Investments in the United States (CFIUS), and the Committee on National Security Systems (CNSS).

The directive would build upon the policy and strategy defined in the National Strategy for Homeland Security, published in July 2002; the National Strategy to Secure Cyberspace, published in February 2003; HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, published on 17 December 2003; and would be consistent with the responsibilities and authorities assigned in the Homeland Security Act of 2002.

In support of this directive, an annual report should be prepared for the president for his approval, including a requirements-driven multi-year-budget, R&D plan, and roles and missions statements for all relevant agencies, including DoD, FBI, CIA, NSA, and DHS.

Conclusion

Thank you for the opportunity to testify before this panel today. I look forward to your questions.