Before the

Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

Committee on Homeland Security

U.S. House of Representatives

Testimony of

Ken Silva

Chairman of the Board

Internet Security Alliance

Washington, D.C.

20 April 2005

Good morning Mr. Chairman. I am Ken Silva. I am the Chief Security Officer and Vice President for Infrastructure Security of VeriSign, Incorporated. I have the privilege of being the Chairman of the Board of the Internet Security Alliance (ISAlliance), on whose behalf I am here today

Before I detail what it is in H.R. 285 that the IS Alliance finds promising, let me tell you a bit more about both the IS Alliance and VeriSign.

Established in April 2001 as collaboration between Carnegie Mellon University and the Electronic Industries Alliance, the IS Alliance is a trade association comprising over 200 member companies spanning four continents. IS Alliance member companies represent a wide diversity of economic sectors including banking, insurance, entertainment, manufacturing, IT, telecommunications, security, and consumer products.

The IS Alliance programs focus exclusively on information security issues. We provide our member companies with a full suite of services including: information sharing, best practice, standard, and certification development, updated risk management tools, model contracts to integrate information technology with legal compliance requirements, and market incentives to motivate an ever-expanding perimeter of security.

Among the IS Alliance's core beliefs are:

First, because the Internet is primarily owned and operated by private organizations, it is the private sector's responsibility to aggressively secure the Internet.

Second, not enough is currently being done by either government or industry to provide adequate information security. This means security not only of the physical and logical elements of the network – but also security of the highly valuable electronic cargo running over the network.
Third, a great deal can be accomplished simply with enhanced technology and greater awareness and training of individuals – from the top corporate executives down to the solitary PC users.

Fourth, while technology, education, and information sharing are critical, they are insufficient to maintain appropriate cybersecurity and respond to an ever-changing technological environment.

Research, aggressive global intelligence gathering, information sharing, and vigorous law enforcement efforts against those who attack our networks are also essential.

Fifth, new and creative structures and incentives may need to evolve to assure adequate and ongoing information security. While government is a critical partner, industry must shoulder a substantial responsibility and demonstrate leadership in this field if we are to eventually succeed.

As Chairman of ISAlliance's Board, one of my roles is to carry these messages not only to government, but also to potential new members of the ISAlliance. When VeriSign helped found the ISAlliance four years ago, there were fewer than a dozen members. But the ISAlliance's key points resonate with ANY organization that uses the information superhighway to conduct its affairs—whether commercial business, academic institution, NGOs, or government. Thus, it is not surprising that, since its inception, the ISAlliance has grown by nearly twenty-fold.

Certainly, my own company, VeriSign takes these principles seriously. VeriSign is a microcosm of the diverse "e" activities on the Internet, of the convergence of the traditional "copper" networks with computer driven digital networks, soon to become the "NGNs" or Next Generation Networks. Commerce, education, government, and recreation all are enabled by the infrastructures and services we and our colleague companies support. VeriSign, the company I am privileged to serve as Chief Security Officer, was founded 10 years ago in Mountain View, California. VeriSign operates the Internet infrastructure systems that manage .com and .net, handling over 14-billion Web and email look-ups every day. We run one of the largest telecom signaling networks in the world, enabling services such as cellular roaming, text messaging, caller ID, and multimedia messaging. We provide managed security services, security consulting, strong authentication solutions, and commerce, email, and anti-phishing security services to over 3,000 enterprises and 400,000 Web sites worldwide. And, in North America alone, we handle over 30 percent of all e-commerce transactions, securely processing $100 million in daily sales.

Of these activities, the one that places us in a very unique position to observe, and to protect the Internet's infrastructure is our role as steward of the .COM and .NET top level domains of the Internet,

and of two of the Internet's 13 global root servers. These are the Internet's electronic "directory" The services VeriSign provides over many hundreds of millions of dollars worth of servers, storage and other infrastructure hardware enables the half trillion daily Internet address lookups generated by all of your web browsing and emails to actually reach their intended destinations. Consequently as the manager of several 24x7 watch centers where our engineering staff observe as these 500 billion daily requests circle the globe, we see when elements of the infrastructure are attacked, impaired, taken off the air for maintenance, or otherwise have their status or performance altered. Because we observe and record this, VeriSign is capable of, and often involved in the identification of the nature, severity, duration, type, and sometimes even source of attacks against the Internet. Our experience in doing this for over a decade, I believe makes VeriSign uniquely interested in how the government architects its companion cybersecurity services.

I am pleased to have the opportunity to speak in support of H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act of 2005; I would like to make three overarching points about the legislation:

First, both the public and private sectors need to become more pro-active with respect to cybersecurity.

A smattering of statistics can briefly outline the growing nature of the growing cyber security problem. According to Carnegie-Mellon University's CERT, there has been an increase of nearly 4000% in computer crime since 1997. The FBI declares Cybercrime to be our nation's fastest growing crimes. One FTC estimate puts the number of Americans who have experienced identity theft at nearly 20 million in the past 2 years, suggesting the link between Cybercrime and identity theft is not merely coincidental. CRS reported last year that the economic loss to companies suffering cyber attacks can be as much as 5% of stock price. Furthermore, the OECD reports that as many as 1 in 10 e-mails are viruses and that every virus launched this year has a zombie network backdoor or Trojan (RAT). Globally they estimate 30% of all users, which would mean more than 200 million PCs worldwide, are controlled by RATs.

Perhaps most ominously, we know from reliable intelligence that terrorist groups are not only using Cybercrime to fund their activities, but are studying how to use information attacks to undermine our critical infrastructures.

Second, the administrative changes and management taskings set out in H.R. 285 must be supported by an adequate level of funding to permit the Department to carry out the critical mandates of this bill.

In particular, cybersecurity research is one area of critical financial need NOT specifically mentioned in the legislation. The basic protocols the Internet is based on are nearly 30 years old; they did not contemplate the security or scale issues we face today and will continue to face in the future. Increasing Federal funding for cybersecurity research and development was recently cited by the President's Information Technology Advisory Committee, (the "PITAC"). After studying the U.S. technology infrastructure for nearly a year, PITAC noted in its report entitled "Cyber Security: A Crisis of Prioritization" that "most support is given to short-term, defense-oriented research, but that little is given to research that would address larger security vulnerabilities." The IS Alliance fully agrees. Substantial funding needs to be provided for basic research in cybersecurity. Industry, itself, can not sustain the level of research investment that is required. The US government must increase its investment.

Third, sufficient REAL authority and trust need to be invested in the person who heads up the Cybersecurity organization within the Department. Without this stature and trust, the elevation of the organization to an "Office" and the bestowing of an Assistant Secretary title will have little benefit. Mr. Chairman, there should be no shame in pointing out what we all know to be true: our economic and national security depends on this job being done right.

"Cybersecurity" means the protection of the physical and logical assets of a complex distributed network comprised of long-haul fiber, large data switching centers, massive electronic storage farms, and other physical assets worth hundreds of billions of dollar; the software programs, engineering protocols, and human capital and expertise which underlie it all are equally valuable. And cybersecurity means protection of the activity—economic and national security—carried on that infrastructure. All of these infrastructure assets combine to support activity that, in the commercial

area alone, account for about $3 trillion dollars daily, according to the Federal Reserve Board. That's $130 billion per hour that depends on a safe, reliable, and available Internet. An infrastructure of such great importance to America's economic and national security demands leadership that is trusted, visible, and effective.

Several provisions of H.R. 285 are of special note:

First, the final section does us all the important service of attempting to define—and to BROADLY define— "cybersecurity", to encompass all of the diverse legacy, present and emerging networked electronic communications tools and systems.

Second, the bill's repeated emphasis on collaboration between the Department and the private sector—in each present and proposed NCSO operational area, as well as across government – reflects a wise understanding of the dynamic nature of the cyber infrastructure, and the diverse interests in and out of government which must cooperate to assure the networks' security and stability. I will address some specifics, as well as IS Alliance's incentives programs, later in my testimony.

Third, in a related area, language in Section 2 (d) directs the consolidation into the NCSO of the existing National Communications System (NCS) and its related NCC industry watch center, which for two decades has provided industry-based alert, warning, and analysis regarding attacks against the traditional telephone networks. These existing important watch functions support critical national security and emergency preparedness communications; their consolidation will bring Departmental practice more inline with emerging technological realities. If done with appropriate care and recognition of the valuable, unique role the NCC has played in supporting NS/EP communications for two decades, consolidation could also make the function stronger and better able to protect these converging assets.

Fourth, the ISAlliance strongly supports voluntary cybersecurity best practices highlighted in section 5(A). We believe that market-driven cyber security is the appropriate model to compel positive cybersecurity improvements within the nation's cyber critical infrastructure. Towards this end, the

insurance industry, among others, have made great strides and continue to advance the state-of-the-art among market-driven cybersecurity best practices.

COMMENTS on SPECIFIC PROVISIONS

Developing new tools to address cyber threats depends on real public-private cooperation. H.R. 285 provides the Department with significant improvements that the ISAlliance believes may help achieve better organization, more cooperation, and greater effectiveness in its collaborations with the industrial, private-sector custodians of the cyber infrastructure, in its cooperation with other agencies of government at the Federal, sub-Federal and international levels, and in its development of new tools to combat cyber threats.

With its focus on government-industry cooperation and cross-governmental cooperation, this bill correctly identifies the two centers of gravity for successfully meeting the cybersecurity challenge. Current programs must continue, which address:

- analysis of threat information;
- detection and warning of attacks against the cyber infrastructure;
- restoration of service after attacks;
- reducing vulnerabilities in exiting network infrastructure, including assessments and risk mitigation programs;
- awareness, education, and training programs on cybersecurity across both the public and private sectors;
- coordination of cybersecurity (as directed by HSPD-7 and the Homeland Security Act) across Federal agencies, and between Federal and sub- federal jurisdictions; and
- international cybersecurity cooperation.

All of these are essential functions. Even in our custodial role for many of the infrastructures that support the $10 trillion U.S.”eConomy”, few would assert that private industry can, or even SHOULD, manage these functions. They are PUBLIC functions, properly performed by government, but in cooperative collaboration—persistent and polite collaboration between government and industry.

I want to note here, Mr. Chairman, that we realize the challenges for DHS/NCSD are far, far easier said than done. Everyone working at the Department, including those in the infrastructure protection and cybersecurity divisions, deserves our sincerest gratitude. I want to personally thank my colleague on the panel today Mr. Yoran, as well as his predecessors, Mr. Clark & Mr. Simmons, as well as his successor Acting Director Purdy. And Mr. Liscouski who oversaw the entire infrastructure division; they all worked, or are working, as hard as they can at an imposing task.

That said however, it is a task that must be completed, no matter how difficult And IS Alliance is not unmindful of cost. But a national cybersecurity awareness and training program as provided by subsection (1) (C), a government cybersecurity program to coordinate and consult with Federal, State, and local governments to enhance their cybersecurity programs as provided by subsection (1) (D), and a national security and international cybersecurity cooperation program as provided by subsection (1)(E) are all important and welcome improvements to the nation's overall cybersecurity posture. Absent adequate funding however, the long-term effectiveness of these critical cybersecurity programs will be uncertain.

Unfortunately, and despite great effort to date, the track-record of the Department and NCSD in achieving even an effective dialogue on how to conduct these essential activities has been spotty and even disappointing.

The provisions of Section 2 of H.R. 285 that direct these specific functions may – hopefully, WILL— jumpstart the collaborations that will rapidly make these programs a reality. America cannot fail in doing these things; a cyber Pearl Harbor is not just a catch phrase, but very much a potential reality. The Department's own "Red Cell" exercises, including a notable one published last September, clearly forecasts "blended" terror attacks against the physical and logical assets of our information networks and institutions that depend on them. Such unavoidably attractive targets have the potential to disrupt economic, social, and government activities at all levels. Improved cyber-resiliency – established in part through effective public-private cooperation such as spelled out in Section 2 of H.R. 285 – is one important step in reducing that threat.

Similarly, cross-agency collaborations within Department components – and with other security and anti-terrorism components of government – is not merely common sense, they are essential. In VeriSign's business, we have had opportunities from time to time to try to "go it alone" and reap the

innovator's premium from the marketplace, or to cooperate with competitors on standards and accessible platforms that grow markets and increase business opportunities for all participants. I can tell you that cooperation and the "rising tide raises all boats" approach is preferable to being the single-handed sailor. In cybersecurity, the expertise of many different agencies— Treasury on financial crimes, or Justice on international frauds—being brought to bear just seems compelling.

Several other provisions of the bill have been long-standing areas of interest to the ISAlliance:

The information sharing provision of HR 285 refers back to Section 214 of the Homeland Security Act; the Department's "Protected Critical Infrastructure Information" program attempting to implement this Congressional mandate is long overdue for reexamination. The "PCII" program, though perhaps well meaning has, rather than encouraging information sharing between industry and the Department, chilled the flow of information. The implementing regulations represent a complex bureaucratic structure that seems more intent on keeping Federal employees from accidentally mishandling information, and thus facing prosecution, rather than encouraging a timely flow of attack and threat information from network custodians to the Department. VeriSign and some of our ISAlliance partners who are members of the IT-ISAC helped draft the original Section 214 of the Homeland Security Act. We are anxious to see it work in a manner consistent with its original Congressional intent and enable information flow that will help respond to attacks, mitigate the damage and, above all, prevent a recurrence.

And, as mentioned earlier, the proposal to merge the watch functions of the NCS into NCSO, and create a single, industry-supported watch effort that covers traditional and IP-based assets is clearly a beneficial way to manage the monitoring of network exploits. However, cyber-security is not the sole mission of the National Communications System. Executive Order (EO) 12472 assigns the NCS with support for critical communications of the President and government including, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget. The NCS was established by EO 12472 as a Federal interagency group assigned national security and emergency preparedness (NS/EP) telecommunications responsibilities throughout the full spectrum of emergencies—disaster and warfare as well as cyber attacks. These responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve improvements in survivability,

interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the Government during any emergency. While this mission does cover the spectrum of cyber-security issues, there is more to the legacy role of the NCS that must not be forgotten or overlooked and from which the NCSO can learn as these functions move forward together.

A key issue is missing from HR. 285, however. Funding for cybersecurity research and development is essential. The Director of the U.K.'s equivalent agency, the NISCC, observed recently that the U.K. alone last year spent 3 times as much on cyber R&D in 2004 as the $68 million spent by the Department and the National Academy's "cyber trust" programs to fund private sector cyber R&D. The United States should not be taking a second place position in the funding of cybersecurity research. While we are benefited by the many investments being made by intelligence and defense agencies that do not appear on such comparative scorecards, R&D to support improved security for the majority privately-held network assets must continue and must grow. In a tech industry where 2-3% is not an unusual R&D budget, the FY 2004 $68 million number is an amount you would expect one $2 billion cyber company to spend on R&D, not the entire government of the country that invented the technology.

We are increasingly seeing the solutions for improved security originating from research outside the United States, with outside investment and ownership in the solutions. Unless the U.S. commits to self-defense, funding the research locally at our universities that will produce solutions to secure our nation's economic infrastructure, we run the risk of having our security developed and managed by others than Americans – and that could be a fragile policy both economically and from the perspective of homeland security. We must figure out a way to invest more to match the clever advances being made by the terrorists who WILL attack these networks.

Finally, let me cite three examples of marketplace incentives that IS Alliance believe promote improved cybersecurity investment by industry: The ISAlliance, together with AIG, have agreed on a program wherein if member companies comply with our published best practices they will be eligible to receive up to 15% off their cyber insurance premiums. Visa, another ISAlliance member company, has developed its KISP program which again uses market entry, in this case the ability of

commercial vendors to use the Visa card, as a motivator to adopt cybersecurity best practices. And the IS Alliance has recently launched its Wholesale Membership Program which allows small companies access to IS Alliance services at virtually no cost, provided their trade associations also comply with IS Alliance criteria.

There is also a role for the government to play in promoting industry cyber security; government should be a critical partner if incentive programs will have their maximum impact. Examples of critical incentive programs include the need to motivate and enhance the insurance industry participation in offering insurance for cyber-security risks, where AIG has been a leader, and the creation of private sector certification programs such as those provided by Visa in its Digital Dozen program. These and several other government incentive programs were highlighted last year in the report of the Corporate Information Security Working Group on Incentives which we commend to the Committee for its consideration

In summary. Mr. Chairman, the challenge of America's—and the rest of the Internet-dependant world's security organizations—like the Department's is threefold:

First, DHS and other government cyber agencies need to understand the architecture of the network today and to recognize its ever-growing diversity and complexity;

Second, cybersecurity agencies need to collaborate with the industries that operate most of these network assets and exchange and understand the information exchanged with industry (including employing the best engineering talent available); and

Third, the cybersecurity agencies here and around the world need to cooperate to respond to threats and attacks against our cyber infrastructure rapidly and effectively.

Mr. Chairman, H.R. 285 moves the Department of Homeland Security in the direction of addressing these three challenges. It is especially helpful simply because it applies more attention to cyber security. ISAlliance members want to work with the Committee and the Department to assure that the good intentions expressed in this document become a reality that strengthens America's ability to

prevent attacks against our networks and to make them strong enough to withstand any attacks that do come our way.

I appreciate the opportunity to bring our views before you today, and I am happy take any questions you may have.

--