Before the

Subcommittee

on Federal Financial Management, Government Information and

International Security

Committee on

Homeland Security and Governmental Affairs

United States Senate

"Cyber Security: Recovery and Reconstitution of Critical Networks"

Statement of

Michael A. Aisenberg, Esq.

Director of Government Relations

VeriSign, Inc.

Washington, D.C.

28 July 2006

Statement of Michael A. Aisenberg, Esq.

Director of Government Relations, VeriSign, Inc.

Mr. Chairman, distinguished members of the Subcommittee, my name is Michael Aisenberg. I am Director of Government Relations at VeriSign, the California-based Internet infrastructure company. I am also Vice Chair of the new IT Sector Coordinating Council, engaging with DHS on cyber security policy, and am chair of the President's NSTAC International Task Force, the ITAA Information Security Committee, and a Board Member of the IT ISAC.

I have a prepared statement which I would ask be included in the record in its entirety. My remarks today are those of VeriSign, as a corporate member of the cyber infrastructure community.

Mr. Chairman, I appear here today after a career of thirty years of translating from the "tech" to the "Congressional." My entire career, including my years in government, has largely been spent working with the legislative and executive branches, on behalf of IT companies.

Today, and for the past six years, I do this work for a core Internet infrastructure company. Based in Mountain View California, VeriSign is a company of over 3500 employees, who operate intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. VeriSign currently secures over 450,000 Web sites with digital certificates—including sites for 93% of the Fortune 500. Today, the VeriSign Secured Seal appears on over 34,000 sites worldwide, a ubiquitous symbol of trust. VeriSign facilitates over 18 billion Internet Domain Name queries every day, and can support many times that amount, should RFID tags replace the current barcode system, filling networks with timely product information. VeriSign operates the largest SS7 network in North America, securely routing 2.7 billion phone connections every day from carrier to carrier, across national boundaries, and between protocols. We are the largest mediator of cellular roaming services in North America, and support cellular carriers with the largest inter carrier billing system. We are deeply involved in the development of policy within our sector and at the national level. Our Chairman, Stratton Sclavos is a member of both the President's Council of Advisors on Science and Technology and the President's National Security Telecommunications Advisory Committee, where I am privileged to chair the newly established International Task Force.

Mr. Chairman, I am pleased to be present with distinguished colleague companies, and in particular, with a representative of the BRT, which has recently published its views on DHS' management of cyber security. This document is important, because its conclusions are largely correct and widely shared.

I would like to make three important points today. First, those who make policy in the United States must understand the economic value and critical interdependencies we have developed on our information networks. Second, we must understand, acknowledge and accommodate to both the global nature of our information networks, and the threats and continuing attacks being mounted against them. Third, the security of our networks, largely owned and operated by the private sector, depends on effective partnership between government security, intelligence, law enforcement and user agencies, and the private sector stewards of these infrastructures.

Allow me to elaborate.

Americans must appreciate and keep a clear focus on the critical economic and national security role which our information networks have come to fulfill over a very short period. In less than two decades, this country has evolved an irreversible dependency, and interdependency by America's banking, finance, transportation, health care, education, power, manufacturing and government services on the networks managed by the companies which make up the IT and telecom sectors.

Each day, 3 trillion dollars worth of economic activity pass over secure Federal financial networks. Securities sales settlements, check clearances, interbank transfers. That is nearly 1/3 of our Gross Domestic Product. If these electronic transactions do not have Internet sites such as NYSE.Net, BankofAmerica.com and Treasury.gov available, secure and running, U.S. economic activity begins to grind to a halt, at the rate of $130 billion dollars per hour.   So cyber security-- the function of safeguarding both the physical and logical infrastructures which enable this economic activity-- is an essential activity of DHS, and of the rest of the U.S. national security community. Cyber security is indeed a responsibility which we all share and in which we all have a stake.

Second, we must lose our cyber nationalism and phony techno-xenophobia. The United States—government and industry--must recognize that these information networks are global, and are managed in increasing measure by interests outside of the control of the U.S. government. At the same time, our networks are being subjected to threats and attacked by actors from around the world.

As we reach 200 million North American Internet users by the end of this decade, the rest of the world will pass two billion users. Unquestioningly, we in the U.S. originated much of the underlying technology, the computer and network hardware, and the complex protocols and network software on which the global network depends. But while we have "carpet bombed" the planet with this technology, we can no longer claim exclusive dominion over it. Networks are largely agnostic about national borders. The U.S.—industry stewards of critical infrastructure and the government-- must work globally within public and private sector mechanisms to evolve governance models which retain necessary and appropriate links between U.S. national security, defense and law enforcement interests, while accommodating the legitimate aspirations of governments and network users around the world to have a stake in the operation and evolution of tools that shape their own social and security futures.

Third, the role of an effective government cyber security actor and government-industry partnership is central to the maintenance of the critical security posture protecting cyber networks. It is important we not lose sight of the BRT report's critical conclusion: we need a much improved cyber security activity, not just in DHS, but across government interests.

The global threats mentioned earlier are not slowing, but accelerating. They are not becoming limited, but rather, are growing in scope and scale. They are not becoming trivial, but much more sophisticated. All of these facts mean the overall risk is growing, and for every security solution we put in place, we can expect our adversaries to develop an attempted "trumping" assault. This is much like a cyber arms race, with no end likely to be achieved.

But the BRT's suggestions about the extent of private industry engagement with DHS, especially over the past eighteen months, are, I believe largely incorrect and out of touch with the facts of important progress being made in public-private collaboration specifically directed at improving the admittedly risky national cyber security environment.

In the last eighteen months, we have seen DHS make significant and important progress in migrating from a frankly dismal posture in 2003-04 when Cyber Security was demoted out of the White House and into the lower rungs of a new agency, to a substantial, active entity engaging effectively with industry on many fronts.

Beginning with the TopOff III exercise planning in the fall of 2004, a steady improvement and expansion of industry involvement with DHS' cyber and network security activities has been evident. This improvement must continue.

The TopOff III exercise occurred in the spring of 2005 with less-than-desirable cyber and telecom sector participation. At about the same time, early drafts of the National Infrastructure Protection Plan or "NIPP", devoid of any meaningful discussion of the cyber infrastructure were released, and thankfully, promptly pulled back. These represent the low points.

Comment from industry on these processes began to be sought by new DHS leadership. Private sector involvement in DHS' policy process from their beginning, rather than at the end, long an aspiration of those of us representing industry through our organizations, began to be practice.

The national cyber security exercise, Cyber Storm, which occurred in February, included extensive sector participation in its planning, and was a remarkable success as a learning experience in public-private cooperation. Led by the IT ISAC, the IT sector gained valuable experience in Cyber Storm, and a new impetus toward the development of a concept of emergency operations for the sector.

DHS' multi stakeholder Internet Disruption Working Group (IDWG) was developed in 2005 and culminated in a day-long planning conference in November, and a recent valuable and widely attended day-long table-top exercise last month, involving DHS and other security agencies, other Federal and sub-Federal government interests and a wide range of private sector cyber infrastructure organizations.

The government's security operations community, GFirst, held its annual conference in Florida in May, which was widely attended by dozens of private sector representatives as well as hundreds of government network security managers, and accompanied by a day long engagement between senior staff or the U.S. CERT and the IT ISAC's con ops task force.

The NIPP has just been released, over the signatures of Secretary Chertoff and 14 other Cabinet members. The NIPP, as a framework for action, including public-private collaboration, incorporates extensive views of the IT and telecoms sectors, and explicitly reflects a focused recognition of the cyber sector's structural and operational differences from physical critical infrastructures, both in the NIPP text and in the separate Cyber Appendix.

The IT and Communications Sector Specific Plans contemplated as operational components of the infrastructure protection process are now under development in a full partnership model between industry representatives and DHS and other GCC member agency representatives. The process is thoughtful, effective, and may well be exemplary for other sectors' SSP development.

These milestones in improvement in the relationship between cyber sector industry interests and the NCSD and NCC staff are important and significant. They are, however, not a solution, but a beginning. This is because cyber security is indeed an ongoing process, and because, as GAO reports so often state, "Progress has been made, but much remains to be done."

Indeed, many of us believe that notwithstanding these improved engagements between the public and private sectors, the actual operational posture of the cyber sector and DHS' is still fraught with risk. It has been observed that if a

9/11 like attack were to take down the NYSE today, (putting aside the issue of improved back-up sites) there is simply no way that the NYSE could restore its network dependent functions in the same four days it did in 2001, and indeed, perhaps not in four weeks.

And the principal reason for this unlikely prompt restoration is DHS, or rather, the bureaucratic impediments to the kind of nimble, self-motivated, selfless action that dozens of private sector entities engaged in 2001 to bring the exchanges back on line. Katrina has amply illustrated these problems; we should not wait for a 2006 hurricane season test of post-Katrina lessons-learned to determine if our economic and other network dependent infrastructures are supported by a necessary government structure, to facilitate private sector action. We need to act without delay to assure that our networks and the critical sectors dependent on them are resilient enough to withstand the attacks being mounted against them each day. And our critical networks must be supported by the appropriate tools from government as well as industry to assure the ability to recover from disabling attacks with minimum collateral impact on our economy and security.

Several steps are necessary to assure this.

First, DHS' modest cyber security budget must be insulated from the continuing reprogramming and budgetary cuts now underway. There will be neither a virtual Bourbon Festival OR Nick's Online Check Cashing if there is no Internet.

Second, a cyber security leader with credibility in industry and within the Federal cyber community must be identified and appointed as DHS' permanent Assistant Secretary for Cyber security and Telecommunications without further delay.

Third, critical R&D projects directed at improving the key security protocols of the Internet must be funded and launched or relaunched, on a fast track basis if possible.

If we do these things, we will not guaranty that our adversaries will stop attacking our critical cyber assets, but we will improve the likelihood that we will successfully withstand those attacks, and retain the availability of these infrastructures on which we are now so dependant. Thank you Mr. Chairman, and Mr. Chairman, I will be happy to answer any questions.