Ken Silva

Testimony Before the
House Homeland Security Committee

April 19, 2007

Good morning, Mr. Chairman and distinguished Members of the Committee. My name is Ken Silva and I serve as Chief Security Officer of VeriSign.

VeriSign operates intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. The company is headquartered in Mountain View, California and it has additional corporate facilities in Virginia, Kansas, Washington state and Massachusetts.

Thank you for the opportunity to testify today. I have a prepared statement, which I would request be inserted in the record.

First, I want to commend and thank you for holding this hearing. All too often, cyber security is only the focus of attention after high-profile incidents. But it's the daily efforts by the government and private sector that ensure that we are prepared so these attacks don't cause significant economic disruption.

And make no mistake about it, cyber attacks occur every day, with increasing frequency, intensity and sophistication. For the most part, Internet users never even know of these incidents because the infrastructure is continually strengthened and fortified to manage them.

While the Internet infrastructure may be invisible to users, its importance cannot be overstated. Internet usage has grown dramatically. The dot-com bust gave the illusion that Internet growth had slowed down, but in fact it has grown at remarkable rates. At the height of the dot-com boom in 2000, for example, roughly 250 million people used the Internet. Today, according to Internet World Stats, more than 1 billion users worldwide rely on the Internet.

The technology of the Internet has transformed personal communications, banking and finance, government process and manufacturing. Twenty-five percent of America's economic value moves over network connections each day. If the Internet were to go down for a just few hours, we would lose hundreds of millions of dollars of economic activity.

For those reasons, it is critical that we make protecting our Internet infrastructure a priority.

As the operator of the .com and .net domain registries as well as the steward for two of the 13 root servers that serve as the nerve center for the Internet infrastructure, VeriSign has a unique position to observe cyber threats.

The scale and scope of cyber attacks has grown dramatically over the last decade. For example, bandwidth demands to deal with cyber attacks have increased 150 times since 2000. A look at the two largest attacks reflects how attacks have increased.

In October 2002, the Internet community got a wake-up call when the 13 DNS root servers, which serve as the heart of the Internet addressing system, came under heavy denial of service (DoS) attack.

While the October 2002 attack slowed down the Internet, it didn't cripple it.

Infrastructure providers took steps to protect the networks to cope with this new threat, in part spurred by concern that terrorists might target the Internet. Significant bandwidth was added to manage future attacks and to decentralize the infrastructure so that a single incident could not knock out a root server. Attacks on the infrastructure did not let up, although the newly fortified system was far better prepared to handle them.

An attack of that scale today is viewed as ordinary and commonplace.

Hackers, however, have become much more sophisticated. A year ago, for example, a hacker systematically disabled over 1,500 websites using approximately 32,000 hijacked PCs. In these attacks, the hacker didn't directly attack the domain-name servers. Instead, they sent their traffic to a legitimate server with a DNS query and a forged source address. This attack was also amplified by 70x.

In an unfortunate twist, the very devices and increased bandwidth that make the Internet more robust and user friendly are being co-opted to compromise the Internet. Now that computers are always-on, they are easily accessible to hackers and other abusers to hijack. The increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure. VeriSign projects that the volume of Internet attacks will increase by 50 percent in both 2007 and 2008. In addition, massive infrastructures such telephony, television, and mobile communications will migrate to the Internet.

We know that the U.S. Government takes Internet attacks very seriously. The Department of Homeland Security conducts "Cyber Storm," the most ambitious cyber wargame of its kind that tests how over one hundred government agencies, organizations and private companies respond to threats to the Internet.

The private sector must also be ready. VeriSign recently announced a global initiative called Project Titan to expand and diversify its Internet infrastructure by ten times by the year 2010.

Under Project Titan, VeriSign expects to:

- Increase its capacity 10 times from 400 billion DNS queries a day to 4 trillion a day. By doing so, VeriSign will ensure that the infrastructure is prepared not only for attacks, but the dramatic increase in Internet usage driven by Internet-enabled mobile devices and social networking applications.

- Substantially expand its infrastructure both domestically and internationally. VeriSign is in process of globally deploying over 70 DNS constellation sites. These sites will distribute Internet traffic and enable us to isolate attacks as they happen.

- Improve the monitoring infrastructure to provide a real-time, in-depth view of anomalous network activity, either malicious or mishap.

Given the increased usage and mounting threats, the Internet infrastructure must be continually fortified. Simply put, if we wait for usage to reach certain levels or attacks to take place to act, we are already too late. While the .com and .net systems currently get more than 30 billion queries a day, VeriSign believes it needs to continue to build a network infrastructure that can support 10 to 100 times that level of volume in the next few years.

What is most concerning now is a scenario where terrorist attacks on a physical structure are combined with a cyber attack. Today is the 12th anniversary of the Oklahoma City bombing that took 168 American lives. If such an attack today was combined with a cyber incident that took down or disrupted our communications networks the damage could be much more severe.

Equally concerning, are the number of more subtle penetration attempts. We are literally constantly probed for vulnerabilities and if we left our guard down for even a few moments, the slightest weakness could be exploited and damage far greater than that of a denial of service attack could occur.

We have all witnessed, and learned, a lot over the last decade. We have had tragic reminders that our critical infrastructure and national symbols are targets. We have seen how not adequately preparing for events can have disastrous consequences.

We know that Internet is often taken for granted. But the operators of that infrastructure must never take it for granted. We must remain vigilant in understanding what is driving the growth of the Internet and the malicious efforts of some who wish to disrupt it.

Thank you for the opportunity to testify here today.

-30-