Ken Silva

Testimony Before the
House Government Reform Committee

October 23, 2007

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

VeriSign operates digital infrastructure that enables and protects 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.

I want to commend and thank you for holding this hearing. It is difficult to overstate the importance of amplifying and expanding our national focus on cybersecurity.

Former national cybersecurity Czar Richard Clarke famously warned of the potential for a "Digital Pearl Harbor," in which critical components of the nation's increasingly vital electronic infrastructure would be brought down by a coordinated electronic attack.

In the years since he expressed his concern, nothing has changed to make it less dire. If anything, the threat grows greater every day, as electronic attackers refine their tools and techniques, and the increasingly ubiquitous Internet becomes an ever more attractive target to wrongdoers.

None of us in government or the private sector can afford to sit still on electronic security. Our defenses must always remain two steps ahead of potential holes and exploits.

If we fail to maintain that focus and determination, we'll be holding a very different sort of hearing in the near future -- one in which we're all called upon to answer the hard questions about why the cornerstone of our digital economy failed, and what we could have done to prevent it.

I've been asked to offer perspective on the efforts VeriSign and the Internet industry are taking to ensure that such a calamity never occurs. And make no mistake; it would be a major catastrophe for the Internet to experience a significant failure.

Approximately twenty-five percent of America's economic value moves over network connections each day. A widespread Internet failure lasting just a few hours would trigger hundreds of millions of dollars in losses. A failure lasting a few days would be equivalent to a massive, nationwide work stoppage capable of crippling the economy.

And it's not just our economy that would suffer. Government agencies at every level rely on the Internet for law enforcement, maintaining national security, serving citizens and even legislating. Try to imagine today's Congress trying to operate without e-mail, Web or any Internet-enabled function, and extrapolate that mess out to the thousands of government agencies at the federal, state and local level that would be impacted by such a loss.

What could cause such a failure? There are two potential scenarios. The first is that we in the Internet community simply fail to expand the Internet infrastructure enough to meet the mounting demands placed upon it. The explosion of Internet-enabled devices and applications – text messaging, music downloads, VoIP, Blackberries and device-to-device communications – has created exponential growth in Internet traffic that far exceeds the traffic increase attributable to new human users. While the number of users has increased 300 percent since 2000, the volume of traffic on .com and .net has increased a stunning1,900 percent over the same period. The good news about this scenario is that it is entirely avoidable, so long as companies like VeriSign continue to invest, in robust, forward-looking improvements to our vital electronic infrastructure.

The second potential for failure is that we fall short in adequate protection our critical resources against the host of increasingly sophisticated cyber attacks being directed against it. As the Internet has evolved, so too have the threats to its continued stability.
The days in which most online troubles were caused by cyber-vandals, defacing popular Web sites for a few moments of fame are long gone. Internet crimes are increasingly conducted by sophisticated international crime syndicates that reap huge profits by targeting the network and its users. Even more frightening is the rise of cyber-attackers backed by governments and other deep-pocketed enemies of the United States.

Electronic threats like SPAM, Phishing, spyware, identity abuse, viral attacks, and denial-of-service exploits -- involving hijacked computers linked through broadband connections, can make use of massive bandwidth to deliver their malicious payloads. A spate of serious attacks last year reflects how these incidents have grown in frequency and sophistication. Today's attacks can cause damage a hundred times more extensive than the attacks of just a year ago.

This is why investment in the infrastructure is critical. Simply put, if we wait for usage to outpace development or for sophisticated attacks to overwhelm our stagnant defenses, we are already too late.

We learned the cost of complacency as a country when we watched the damage done by Hurricane Katrina. By the time Katrina hit the Gulf Coast, it was too late to strengthen the levies. We should not have to learn that lesson more than once. Critical Resources should be reinforced way before there is a threat to their well being.

The Internet continues to grow at dramatic rates, which means the infrastructure must scale to meet that demand. No one can take security and stability of these networks for granted; not VeriSign, not the ISP's or the other private sector players and certainly not the government, .

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 of the Internet, VeriSign understands what's at stake. Over the last eight years, VeriSign has operated its infrastructure with 100 percent uptime – in other words, the systems that ensure the Internet's core infrastructure remain functional has never gone down.

VeriSign's primary computers that handle the .com and .net traffic are now capable of handling 10,000 times the DNS query volume they could handle in 2000. To put that in perspective, although that Moore's Law states that computing power doubles every 18 months, we have chosen to increase our capacity at 600 times that rate.

And while the .com and .net systems currently get more than 30 billion queries a day, we will need to build a network infrastructure that can support 10 to 100 times that level of volume in the next few years.

That is why earlier this year VeriSign announced a global initiative called Project Titan to expand and diversify its Internet infrastructure by to be ten times more robust by the year 2010. Under Project Titan, VeriSign is:

- Increasing its capacity ten 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 expanding 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.

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

These upgrades are vital to managing the surge in Internet interactions and protecting against cyber attacks. VeriSign is well on its way to meeting its goals under Project Titan and is already considering how to address the next set of challenges.

I often get asked what about Internet security keeps me up at night.

I always say there are two things. The first is the volume and sophistication of attacks. The very devices and increased bandwidth that make the Internet more robust and user friendly are being deployed every moment of every day to compromise the Internet. Now that computers are always on, they are much more easily hijacked and turned to malicious ends by hackers and other abusers. And 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. What deeply concerns me is a scenario in which terrorist attacks on a physical structure are combined with a cyber attack. Equally concerning, are the number of more subtle penetration attempts. We are literally constantly probed for vulnerabilities. If we let our guard down for even a few moments, the slightest weakness could be exploited to inflict damage far greater than that caused by a traditional denial-of-service-attack.

The second is the potential for what I call a well-meaning, self-inflicted wound. As we make vital improvements to build out the infrastructure and expand the Internet we must be careful that our efforts don't inadvertently Balkanize the network or confuse users.

The Internet community is currently discussing the important issue of Internationalized Domain Names (IDNs). These are domain names that can be entered using the letters or characters of local languages, such as Mandarin. This is an important step that can open up the Internet in new ways and to billions of users around the world. But implementing IDNs in a stable, secure manner requires resolving a host of technical and business issues . If we don't handle this issue correctly, we could create separate and confusing Internet "rules" that confuse Internet users. Worse, we could create the opportunity for oppressive regimes to establish new conditions on businesses impacting their

ability to realize the full potential of the Internet as a tool to promote openness and commerce.

Whether it's fortifying the infrastructure against cyber attacks or creating a framework to truly internationalize the Internet, it is vital that government and private industry take "long view" with a goal towards ensuring security, stability and user confidence that the Internet will continue to function as well or better than it has in the past.

As a steward of the Internet infrastructure, it is our job to ensure that the Internet remains reliable and always on and therefore available so that e-commerce flows, emails are delivered and users can visit the Web sites they want, whether they are at home or half-way around the globe.

To do so, the private sector must stay a step ahead of demand and the next wave of threats. The operators of this infrastructure must never take it for granted. We must be vigilant in understanding what is driving the growth of the Internet and the malicious efforts of those who wish to disrupt it.

Thank you for the opportunity to testify here today.

-30-