

**Ken Silva**

**Testimony Before the  
House Energy and Commerce Subcommittee on Communications,  
Technology, and the Internet**

**June 4, 2009**

Good morning, Chairman Boucher, Ranking Member Stearns and distinguished Members of the Subcommittee. My name is Ken Silva and I serve as Chief Technology Officer of VeriSign.

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

By way of background, 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, Delaware and Massachusetts.

I want to commend and thank you for holding this hearing. At a time of economic challenges and uncertainty, it would be easy to focus on the many pressing near-term issues that affect our nation. But it is critical that we also focus on the Internet, because the infrastructure is not only integral to the economic recovery of our country, but to our national security as well.

Simply put, the Internet is now the platform for an enormous portion of our economic activity, our entertainment and communications. President Obama put it best last week when he said. "None of these 21st century challenges can be fully met, without America's digital infrastructure -- the backbone that underpins a prosperous economy and a strong military and an open and efficient government. Without that foundation we can't get the job done."

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 understands what's at stake. Over the last 10 years, VeriSign has operated its infrastructure with 100% uptime – in other words, the systems that ensure the Internet is functional have never gone down.

But the Internet is not a static system. It's a dynamic and continually changing network of networks.

It is growing dramatically overseas, raising questions about its future governance and the role of nations who may not share our values about freedom of expression, content and commerce.

It is increasingly relied upon by citizens, businesses, organizations and governments, raising questions about whether it can continue to scale to meet the needs of over 2 billion global users, increasingly rely it upon.

It is the target of attacks that expand exponentially in volume, scope and sophistication. Some have raised questions if enough is being done to protect the critical networks that serve as a lifeline for commerce and communications.

I would like to address all three of these challenges in my testimony.

### Internet Governance

When it became clear that the Internet would have a profound impact on every facet of society, the Clinton Administration took the lead in establishing ICANN to serve as the technical coordination body. The Department of Commerce was given the task of helping guide ICANN and provide a governmental “backstop” to the global Internet community.

More than a decade later, ICANN has continued to grow and develop. It has not been without its challenges, or issues with the Internet community, but it has served an important role in creating stability with the community. Now the Internet community has grown to every corner of the globe, prompting questions about whether the Commerce Department, or any one government, should serve as that backstop.

As policymakers around the world grapple with that question, we believe that must consider how to ensure that the Internet, and the community that guides it, are insulated as much as possible from domestic political pressures or the goals of those in the world who, in the name of stability, want to restrict what has made the Internet so dynamic – namely its innovative force.

With that, we look forward to the outcome of the discussions between ICANN and the Department of Commerce over the Joint Partnership Agreement (JPA), particularly as it relates to its impact on the security and stability of the Internet and its responsible stewardship.

From our point of view, while ICANN has continued to make progress in certain areas since these recent public proceedings, the basic circumstances giving rise to widespread community concerns over an expiration of the JPA remain largely unchanged and further progress is critical prior to an expiration of the agreement and end to all governmental oversight of ICANN.

Among the issues we know being discussed are how to continue to ensure that the goals of accountability and transparency continue to be worked on throughout the ICANN process. The overall goal in this process must be the strengthening of the security and stability of the Internet.

## Scaling the Internet

Because the Internet never goes down, users, and even some companies who rely on it for their business model, take it for granted. But VeriSign, other private sector players and governments cannot take security and stability for granted. We must continually invest and work to improve its capacity.

To keep up with the demand, VeriSign's primary computers managing .com and .net traffic can now handle more than 10,000 times the DNS query volume they could handle in the year 2000. To put that in perspective, that increase is 600 times greater than Moore's Law, the theory that computing power doubles every 18 months.

Two years ago, the .com and .net systems handled more than 30 billion queries a day. Today, they handle more than 50 billion queries a day – a 67 percent increase in just two years. In other words, DNS capacity is increasing at a rate that is 3 times faster than domain name registrations. VeriSign is committed to building a network infrastructure that can support up to 100 times that level of volume in the next few years.

That is why VeriSign launched a global initiative called Project Titan to expand and diversify its Internet infrastructure by ten times by the year 2010. These investments include increasing capacity 10 times over, from 400 billion DNS queries a day to 4 trillion DNS queries a day to prepare for attacks and new usage that continues to increase daily. We have also expanded our infrastructure both domestically and internationally through the deployment of over 70 DNS constellation sites that ensure that attacks can be isolated and Internet traffic is not disrupted.

Even this is not enough. We are now in intense discussions about what the future of the Internet will look like and how the infrastructure must be fortified and adapted to ensure it can keep up with those changes.

## Securing the Internet

President Obama's order that his new cyber security czar sit on his National Economic Council and National Security Council underscores the threat that cyber attacks pose to our nation.

As Chief Technology Officer I have had to identify and manage attacks every day. Cyber criminals cleverly manipulate the Internet's advances. The growth in the number of computers world wide means that more devices can be turned into botnets to stage attacks on corporate networks. Now that computers are always-on, they are more easily accessible to hackers and other bad actors to hijack. And the increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure.

There are many issues that we must address as an Internet community. We must resolve the issue of creating internationalized domain names while ensuring that they are technically stable and provide a consistent Internet experience for users around the world. We must continue to invest and deploy infrastructure upgrades such as DNSSEC and IPv6 in a way that is least disruptive to Internet users, developers, businesses and governments.

What we cannot afford is to play politics with the Internet infrastructure. We must continue to work together to invest and develop the infrastructure so that it can continue its role as a platform for commerce and communications.

I know that VeriSign, ICANN and the rest of the Internet community will work diligently to ensure that the infrastructure remains reliable and secure.

Thank you very much for your time.