

**Testimony of
Roger J. Cochetti
Senior Vice President and Chief Policy Officer
VeriSign, Inc.**

**Before the
Subcommittee on Science, Technology and Space
U.S. Senate Committee on
Commerce, Science and Transportation**

December 5, 2001

Mister Chairman, Members of the Subcommittee:

My name is Roger Cochetti. I am Senior Vice President-Policy and Chief Policy Officer of VeriSign, Incorporated. I am pleased to be here today to address the issue of the security of the Internet in the context of Homeland Security and the aftermath of the September 11th terrorist attacks.

It is particularly appropriate, Mr. Chairman, that VeriSign participate in today's hearings because we are the premier trust company on the Internet and, perhaps more than any other company that one can think of, we are concerned about the security of the Internet. VeriSign offers critically important Digital Trust Services, which include the most important elements of the Internet's domain name system (called the DNS), secure authentication services (in the form of digital certificates called digital signatures) and payment services for Web-based merchants. In fact, we are the world's leading provider of domain name, electronic authentication and Web merchant payment services, which together make up essential elements of the Internet's infrastructure and without which, the medium as we know it, could not function.

As the 1997 Report of the President's Commission on Critical Infrastructure Protection observed, the Internet has emerged as a single pervasive infrastructure technology relied on by every other keystone segment of our economy—financial services, electric power, water, health care, manufacturing, transportation and telecommunications. Accordingly, all of us in VeriSign are acutely aware of the

millions of retail merchants, universities, banks, businesses, libraries, museums, government agencies, civic organizations, and just plain families and individuals who rely on our facilities and services billions of times each day. And we are acutely aware of our responsibility to maintain those facilities and services at the highest possible level of reliability.

Because of our unique and highly trusted role in making e-commerce and the Internet work, we have had a long-standing and fundamental commitment to security. Thus, for us, the tragic events of September 11th provided a sad confirmation that our attention to security had not been misplaced. They also served as a reminder that our concern for security must be constantly refreshed and proliferated through out the Internet economy.

QUESTIONS POSED

In the Subcommittee’s hearing announcement, Mr. Chairman, you have asked us to focus on a series of questions directed at the physical technology infrastructure resources—how they were impacted by September 11th, whether a corps of industry experts would benefit the response or aid in mitigating the impact of any future episodes, the usefulness of caches of spare supplies of technology appliances like cell phones and laptops, what other benefits might be derived from such preventive measures and organization.

As the Subcommittee knows, the World Wide Web operates in a hierarchical structure, with Top Level Domains (TLDs) serving as the main divisions among Websites. Domain names serve as the directories for the Internet and the Domain Name System (DNS) is sometimes described as the “air traffic control system of the Internet.” TLDs include the ubiquitous dot com/net/org, such well-recognized domains as dot gov or dot edu, and more than 240 country code TLDs, such as dot us or dot uk.

The directory of all of these TLDs is created and distributed in a network called the Internet’s Root Servers, and we operate the primary of these root servers, the so-called “A Root”, which has been described as the single point where the entire Internet comes together. The authoritative list of the Internet’s TLDs originates in our A Root and from there it is distributed to other root servers, including our own, around the world.

In addition, we operate the largest and most popular top level domains on the Internet, .com, .net, and .org, through a network of our own servers in North America, Asia, and Europe. Finally, we operate a number of smaller domains, such as .edu, typically under contract to the organization that is that domain's legal registry operator. In all of these DNS functions, we ensure that the Internet's DNS is available and reliable, notwithstanding both its dramatic growth (we now process more than 5 billion communications and transactions daily) and frequent unintentional and intentional threats to its operational stability.

Because VeriSign operates in this aspect of the domain name system at the highest level of the Internet's architecture and because many of the most serious threats to the security of the Internet occur at the level of the network or Website operator, we cannot claim to have a close view of some of the Internet's most vulnerable elements. It is clear to us, however, that all elements of the Internet, but most particularly network and Website operators who are the most at risk, would benefit from some form of catalogue of experts and reservoir of equipment. So, our short answer to the Committee's questions is generally "yes, it would be useful to pursue something like what has been raised"

On the other hand, it would be impossible to predict that either a catalogue of experts or a cache of supplies will be necessary or useful in the event of any future emergencies, since so much depends on the context and circumstances.

BACKGROUND TO THE DNS

Thirty years ago, the U.S. Government began research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of Defense's Advanced Research Projects Agency (DARPA) in the 1960s. ARPANET was later linked to other networks established by other government agencies, universities and research facilities and during the 1970s, DARPA also funded the development of a "network of networks;" which later became known as the Internet. The protocols that allowed the networks to intercommunicate became known as Internet protocols (IP).

Until the early 1980s, the Internet was managed by DARPA, and used primarily for research purposes. Nonetheless, the task of maintaining the name list became onerous, and the Domain Name System (DNS) was developed to improve the process. Also, during this time, management of the network was passed from DARPA to the National Science Foundation (NSF), which referred to the medium as the NSFNET.

In 1992, the NSF entered into a Cooperative Agreement with Network Solutions, Inc. (NSI), which company was subsequently acquired by and merged into VeriSign. Under the Cooperative Agreement, NSI (now VeriSign) provided a variety of DNS services, including the domain name registration services and the operation of key parts of the Internet Root. Also in 1992, the U.S. Congress gave NSF statutory authority to allow commercial activity on the NSFNET. This facilitated connections between NSFNET

and newly forming commercial network service providers, paving the way for today's Internet.

In 1998 and 1999, after authority over the Cooperative Agreement had transferred from NSF to the Department of Commerce, amendments were negotiated which introduced a new entity into the management of the DNS, the ICANN, and which introduced competition at the retail registration level for .COM, .NET and .ORG names. In the spring of 2001, the agreements between the Department and VeriSign, the Department and ICANN, and VeriSign and ICANN were substantially modified and extended; and later this year, new TLDs --such as dot info-- were introduced. All of this against the backdrop of dramatic growth in the use of country TLDs, such as dot de and dot uk.

VERISIGN AND INTERNET SECURITY

While the Internet has changed quite a bit since VeriSign (through NSI) first assumed responsibility for major parts of the DNS in 1992, one thing has not changed much at all: The trust that others have placed in VeriSign and our commitment to the highest level of reliability. This is equally true of our digital signature services --on which hundreds of millions of dollars worth of transactions rely—as it is our domain name services --on which hundreds of millions of users rely. We bring that same commitment to our payment services and our expansion into new Internet services.

For example, in our operation of the dot com TLD, our standard of performance is such that we view the traditional “six-sigma” 99.9999% accuracy as insufficient, since it would permit some 40 bad Internet connections daily. If of those occurred on a site like aol.com or Amazon.com, the consequences could be significant. And so, that level of error is simply, for us, unacceptably high.

To engineer a secure system with the level of accuracy and stability required for a nearly error-free Internet is costly and complex. Unlike most other networking challenges, it cannot be shared with our clients and customers, whose technology investment need only be quite modest by comparison to fulfill their role as an ISP or a network operator. Unfortunately, this disparity can exist not only in required investment in physical infrastructure, but sometimes in security practices as well.

SINCE SEPTEMBER 11th

As I mentioned earlier, the sad events of September 11th proved, if it was needed, that we must both prepare and carefully plan for security threats. Since then, we have expanded our efforts to reach out to both government and others in our industry and share both our experience and accumulated knowledge in this area.

Among the areas that we think deserve continued, priority attention are:

- 1) We must, as the White House has now done, identify this as an area of priority concern; and
- 2) We must, as the White House is now doing, develop a strategy for how to address threats at all levels to the Internet; and
- 3) We must closely monitor the infrastructure and seek early detection of threats to its operational stability.

Finally, in addition to the very important ideas that the Subcommittee is already considering, we would encourage the following steps:

- 1) The enactment of legislation that would reduce some of the risks incurred by companies if they share sensitive network information with Federal agencies concerned about security.
- 2) The wider use of security audits both among Federal agencies and Federal contractors.
- 3) The strengthening of various Federal consultative mechanisms that permit information sharing between the private sector and agencies concerned with Internet security.
- 4) Federal support for the wider use of both encryption and PKI-based authentication tools, which together can help ensure a significant increase in the general security of both the Internet and of e-commerce and e-government.

In conclusion, Mr. Chairman, let me say that the events of September 11th were pivotal

for the Internet, as they were for almost every other major element in our society and economy. Fortunately, the Internet's core infrastructure, including the DNS, operated without interruption. But September 11th serves as a reminder that the next threat may not be so easily contained and it is for that threat that we must be prepared.