BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

COMMITTEE ON GOVERNMENTAL REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

TESTIMONY OF

KENNETH SILVA
VICE PRESIDENT

VERISIGN, INC.
DULLES, VIRGINIA

10 SEPTEMBER 2003

Good Morning Chairman Putnam and members of the Subcommittee. My name is Ken Silva. I am Vice President for Networks and Security of VeriSign, headquartered in Mountain View, California.

VeriSign is pleased to have the opportunity to provide our views on what we believe is one of the most important, yet poorly understood phenomena facing our nation—the epidemic of virus and worm attacks that continue to threaten the integrity and security of the information networks on which we have all come to depend.

VeriSign as a company is perhaps uniquely situated to observe the continuing assaults on our information infrastructure. Our company provides industry-leading technologies in three relatively distinct—yet interrelated -- lines of business. Each of the three serves an important role in the rapidly converging infrastructures that support communication and electronic commerce around the globe.

VeriSign's Telecommunications Services group provides the essential signaling and switching services that make today's digital telephony -- ---both wired and cellular—possible. This includes features like call waiting and forwarding, wireless roaming and the soon-to-be available wireless number portability.

Our Security organization provides authentication, encryption, secure credit card processing, fraud prevention and detection, managed network security services and a range of other services that enable eCommerce, eGovernment and the over-all secure Internet

experience that hundreds of millions of users around the globe have come to rely on.

Our third major line of business is now known as “naming and directory services”, and includes VeriSign’s assets dedicated to the management of the Domain Name system of the Internet, including our stewardship of the A- and J- root servers—two of the thirteen computers around the globe that represent the top of the pyramid of the Internet’s dispersed hierarchy. This is the part of the Internet’s infrastructure that allows you to type in “www.house.gov” into your web browser and immediately be directed to one unique computer from among the hundreds of millions on the network. In addition, under a contract with the Department of Commerce, VeriSign and it’s predecessor subsidiary, Network Solutions have for over a decade managed the .COM and .NET top level domains that for many have come to symbolize the essence of the net. Figure 1 (attached) depicts the global distribution of these assets.

I have been privileged to serve Network Solutions and now VeriSign since 2000 as manager of the resources dedicated to maintaining the security of these complex technology assets. On behalf of VeriSign, I also serve in a number of industry capacities, including representing VeriSign on working groups of the President’s National Security Telecommunications Advisory Committee—the “NSTAC”, working groups of the NRIC which advises the FCC, and as a Board member of both the Internet Security Alliance and the “IT ISAC”—the IT sector’s Information Sharing and Analysis Center.

I want to make three key points today that I believe are critical to how the Congress and the rest of the policy community deal with the challenges that continuing attacks against our networks pose.

First, we should not underestimate the significance of these attacks. Although the most recent worms and viruses have been labeled non-destructive, they have cost American business in excess of $3.5 Billion in August alone. We can only imagine the cost had these worms actually destroyed valuable data along their path. While it is important to maintain vigilance for state sponsored or terrorist related attacks, many of these attacks have proven to be the work of individuals barely of legal age, or younger.

Second, we must all accept our shared responsibilities. Each of us has a responsibility. This includes lawmakers, government agencies, industry, and private citizens. Government has a role both as a model of secure practices, as well as a thought leader in global security. Our citizens must be educated. We teach our children how to use computers in school, but do we teach them how to use them responsibly and safely? This responsibility for addressing the gap in security awareness is shared by government, industry and families. But at the same time, the challenge to industry of the National Strategy to Secure Cyber Space to exercise leadership in security awareness, education, assessment and practice must be taken to heart by all of us in the Internet business.

Third, we must resist the temptation to demonize software vendors and other members of the network community. The finger pointing is often misplaced and in most cases does more harm than good. It is all too easy to blame the operating system manufacturer for flaws in their code, or the network providers for not securing their networks. Many of the worms attack not only popular operating systems, but open source software and systems as well. Of greater concern to VeriSign as a security vendor are the anecdotes reported in the media; the overreactions these stories may stimulate—by well meaning legislators or others may result in inappropriately large solutions being applied to problems more readily managed narrowly—and by the marketplace.

VeriSign believes there are actions that over time will improve the overall health and well being of the Internet, but there are no magic solutions or silver bullets. Long term health and well being will take time and everyone's efforts. Again, this is as much a responsibility of people as it is of technology.

Because of VeriSign's obligations with respect to the A and J-ROOT servers, we have invested significant power into our infrastructure. Not only do we invest in state of the art hardware and software, we maintain a highly qualified security staff as well. This infrastructure supports not only the security of our services, but those of our security services customers as well. We are acutely aware of what we can do, what we choose to do, and what we choose not to do. For example, we do not manufacture firewalls or anti-virus software.

Instead we choose to rely on other vendors for that. We choose to select vendors that meet our high security and reliability standards and we run through real-world scenarios. Not all vendors pass this test.

We maintain laboratories where we can test security and stability functionality in the protocols and software that we rely upon. These include the protocols used to carry the Domain Name System, the Secure Sockets Layer, and the databases we select. We do this by subjecting them to various assaults and measure the response. We calculate how we can respond to them and we devise strategies for dealing with real-world scenarios. We also work very closely with respected outside sources such as the one operated by my good friend Rich Pethia from the CERT at Carnegie Mellon University. Armed with this information, we can deploy, and advise others on deploying the best configurations.

In addition to software research, VeriSign invests an enormous amount of money and resources into our monitoring capabilities. These monitors are not unlike the telemetry data carried on satellites and weapons systems. They monitor every aspect of our systems and alert us to changes within the system. They allow us to learn from failures and obtain root cause for each incident. Indeed, this monitoring has allowed us to watch some worms propagate throughout the Internet. Figure 2 (attached) depicts the spread and corresponding stress imposed on one of our key assets by the

Sobig.F worm. This picture is from our monitoring system on 19 August, 2003.

Immediately following 9/11, we made some of our monitors available to the National Communications System (NCS) in the Department of Defense. We also made it available to the FBI through the National Infrastructure Protection Center (NIPC). We were somewhat surprised to learn that despite their role in protecting the infrastructure, our security agencies had no such tools at that time. Since that time however, these agencies have undergone many of their own security efforts, both through their own development as well as partnerships with industry

VeriSign's sharing of network information and tools has not been limited to the government—as I noted, we have had a long and close working relationship with the CERT at Carnegie-Mellon University and other academic security centers, and are a founding member of the IT-ISAC, and the NCS' Telecommunications ISAC—both attack information sharing bodies comprised of industry members from the IT and telecommunications sectors.

Because of this investment, we are often the first to notice significant events. On 21 October, 2002, we were the first to notice what was hailed as "the largest Distributed Denial of Service attack ever to hit the Internet". We detected this attack, devised a mitigation strategy and alerted the other ROOT operators, as well as CERT, the CIPB, NIPC, and NCS on its effects, and the countermeasures used to

thwart it. Despite the fact that 8 of the 13 ROOT servers experienced some level of failure, the Internet continued to function without incident to hundreds of millions of users worldwide.

These incidents, as well as the most recent Sobig.F, Nachi, and Blaster worms reveal fundamental truths about the networks and the impacts we experience. Sobig.F for example has increased load to one of resources by as much as 35 times. We should all ask ourselves; do all of our network elements have the requisite capacity to withstand a 35-fold increase in traffic? This would of course include our mail servers, web servers, Internet backbones, etc.

We must assess our adversaries. They prey not only on the weaknesses of software and operating systems, but the predictability of human beings. Sobig did not launch itself. Someone opened it. And to this day, despite all of the press this has received, it continues to get re-launched by unwitting individual users every day. Just a few years ago, worms used to take weeks or months to propagate. Today they take but a few hours to infect the entire world. And, as you have heard from others here today, these weapons are behaving more aggressively and they are increasing their uniqueness. This makes selection of appropriate counter-measures difficult and uncertain.

We all recognize the extent that we rely on our networks for economic activity of every flavor. This includes education, entertainment, health care and government services at every level. VeriSign believes we

must all also face up to the reality that these virus and worm attacks and other “logical” assaults on our information networks are every bit as threatening as physical attacks on our critical infrastructures. These assaults warrant serious attention from every community of interest to discover the strategies needed to defend against them and remedy their impact.

To date, we continue to see the remnants of long forgotten worms such as Code Red, Nimda, and others. This is long after the patches and well-publicized fixes for these worms. In fact, the fix for Blaster (and all of its variants) was released by Microsoft several weeks ahead of the actual worm. These were well known vulnerabilities that the vendor had long since fixed. It was, and is still, the inaction of administrators and home users to remedy these vulnerabilities that these attacks were able to launch. Although technology can do a lot to help in these situations, we cannot ignore the area between the keyboard and the back of the chair. Users are still the weakest link in network security.

The impact of these worms continues to grow with each new worm. Some ISPs are still dropping packets and exhibiting degraded service because of Blaster and Sobig. The network will continue to weaken a little more with each new worm and it’s remnants long after the media stops reporting on it.

But the insidious impact of these attacks is not limited to infrastructure asset compromise or network resource consumption.

In point of fact, there is measurable economic harm being visited on all of the network infrastructure stewards. This harm consists not only of the episodic costs, such as the $3.5 billion cited in August of this year alone, but the long term institutional costs as well. This harm flows downstream to all of the other key economic infrastructures that depend on the Internet.

VeriSign recognizes and believe the assertions by Chairman Greenspan and others about the enormous productivity gains in the past decade attributable to the wide deployment of Information Technology in our economy. Unfortunately, these gains have their own price, which we have not fully understood, and certainly not yet paid—in terms of obligations of appropriate use—including appropriate security practices.

We have had estimates that economy wide, the price tag of universal deployment of adequate minimum security tools across all North American users, in a perhaps three year period of effort, could reach $450 billion—roughly equivalent to the $450 billion per year value assigned to the "information economy." Clearly, we have not reckoned with who—or how—we could pay the price to make such massive network wide investments—or, indeed, who SHOULD ultimately bear this enormous unfunded societal cost.

The most important thing to remember is that securing our network assets is a shared responsibility for all of us. At the most basic level, every individual user can contribute to improve security by taking

basic steps towards improved security hygiene. The prescriptions are well known and widely distributed—yet far too few actually engage even in the most simple, low cost and no-cost measures:

--Use passwords, and change them regularly
--Use antivirus software and update is regularly
-- Patch the operating systems
-- If you have firewall capability, use it; if you don't, get it
-- If you have an "always-on" network connection (such as DSL, or Cable modem), turn it off when you're not using it.

These simple, low cost measures are not a prescription for guaranteed network security. But they are examples of easy steps every user can take to increase their own security posture. By doing so, we improve the overall resilience of the network to attacks. Such measures will strengthen the network's weakest links, and those exploited by attackers.

When taken, these steps reduce the population of target computers a virus can successfully invade. We all benefit as the Internet becomes less hospitable to hackers, spammers or others who lurk in its murky corners. These weakness in security have been exploited by organized crime, nuisance mongers, delinquent youths, terrorists and foreign adversaries. All of these adversaries understand our growing individual reliance and the dependence of key global infrastructures on the Internet. Many of them would exploit present vulnerabilities in order to harm America.

Undoubtedly, every operating system, every Web browser and every email client application in use today could have some additional security feature embedded that it lacked at release. But until users---major network managers at large ISPs, corporate networks and many, many Federal agencies-- demonstrate their full compliance with the version and patch management obligations of their software licenses, blaming their vendors for the extent of virus impact is misplaced and distracts us from the important work at hand.

Mr. Chairman, thank you for giving me the opportunity to appear before you today.