VeriSign, Inc., headquartered in Mountain View, California, is a leading provider of commercial digital trust services that enable Web site owners, enterprises, communications service providers, electronic commerce, or e-commerce, service providers and individuals to engage in secured digital commerce and communications. Our digital trust services include three core offerings: managed security and network services, registry and telecommunications services, and Web presence and trust services. We market our products and services through our direct sales force, telesales operations, member organizations in our global affiliate network, value added resellers, service providers and our Web sites.

VeriSign's Managed Security and Network Services

Managed Security and Network Services include our traditional public key infrastructure, or PKI, services for enterprises or members of our VeriSign Affiliate program, enterprise consulting and management services, digital brand management services and managed domain name services, or DNS. Several of these are of interest in the context of this proceeding.

VeriSign PKI Services. VeriSign PKI Services are sold under the VeriSign OnSite and VeriSign Go Secure! brands, and can be tailored to meet the specific needs of enterprises that wish to issue digital certificates to employees, customers or trading partners.

OnSite Services. OnSite is a managed service that allows an organization to use our trusted data processing infrastructure to develop and deploy customized digital certificate services for its user communities. OnSite can be used by our customers to provide digital certificates for a variety of applications, including, but not limited to: controlling access to sensitive data and account information, enabling digitally-signed e-mail, encryption of e-mail, or secure socket layer sessions. OnSite services can help customers create an online electronic trading community, manage supply chain interaction or facilitate and protect online credit card transactions.

Go Secure! Services. Go Secure! Services are a set of managed application services that enable enterprises to quickly build digital certificate-based security into their off-the-shelf transaction and communication applications. Go Secure! Services complement our OnSite services and are designed to incorporate digital certificates into existing applications such as e-mail, browser, directory and virtual private network devices as well as other devices.

VeriSign Affiliate PKI Services. VeriSign Affiliate PKI Services are sold to a wide variety of entities, which are unaffiliated with VeriSign, that provide large-scale electronic commerce and communications services over wired and wireless Internet Protocol, or IP, networks. We designate these types of organizations as "VeriSign Affiliates" and provide them with a combination of technology, support and marketing services to facilitate their initial deployment and on-going delivery of digital certificate services.

1. The Current State of Information Security

* What are the security risks facing consumers?

The risks faced by on-line consumers have, in the past, been largely described as centering a the destruction, theft, or other compromise of individual Internet users' personally identifiable information, which could lead to or become a part of a theft of money from a financial institution account, identity theft, or some other financial crime. In the post-September 11 environment, care must be taken not to underestimate the potential for harm arising to consumers not as a result of individual action being taken against them, but as a result of some more general exploit against institutions with which consumers have a relationship or on which they may depend, such as a general attack on financial institutions or their critical infrastructure. These are, of course, risks that are largely outside of the consumers' capacity to anticipate or defend against, short of cessation of dealing with such institutions.

Additionally, recent thinking about cyber risks generally has evolved beyond intentional external attacks, to an analysis of derivative risks, resulting from vulnerabilities embedded in the architecture of networks on which institutions upon which consumers rely depend for delivery of their network services. These risks include widely deployed network protocols that may have embedded vulnerabilities, lack of effective security hygiene by institutions or their network providers, and physical vulnerabilities, such as concentrations of hardware in 'single points of failure.

* Are consumers aware of the risks?

Many of these "embedded" risks have become the subject of commentary and discussion as the post-September 11 efforts to respond to threats and improve security have advanced. Even knowledgeable technical experts continue to invest in advancing their understanding of these risks and processes are evolving for sharing information between industry technology experts, law enforcement and the user communities.

* What are the costs to consumers of security measures and of security failures?

Many elements of fundamental security hygiene are available to individual consumers with minimal or no cost. Protecting and changing passwords regularly, turning off unused network connections, or deploying embedded password routines in operating systems all carry no financial cost. Utilizing ISPs that declare their use of security practices, rather than those who do not employ such practices may carry some limited cost, but provide a commensurate benefit.

* Do consumers accurately assess security risks?
* How does consumers' security affect the network as a whole?

The impact of consumers' security - or more precisely - lack of security, to the network as a whole can be assessed from at least two perspectives. The first is aggregate: the network provides an "attractive nuisance" to criminals and exploiters if the extent of security ignorance is widespread and the lack of appropriate self-defensive hygiene is well known. If more individual network users deployed

basic security techniques, there would be less of a fruitful target environment for criminals. The second perspective is derivative: if consumers demanded that their network service providers and correspondent institutions maintained state-of-the-art security tools and practices, the marketplace would select in favor of best-practice providers, and the risk to individual consumers would diminish. For example, it has been nearly two years since the Congress adopted the Electronic Signatures legislation known as eSign, yet the rate of commercial deployment of electronic authentication technologies such as PKI (public key infrastructure) in the commercial eCommerce marketplace has not accelerated appreciably, even though this was the intent of the legislation's proponents. (A reluctance of some institutions to invest in PKI – what is described by at least one senior government technical official as the "gold standard" for authentication of identity and encrypted security of network content – may be best explained by misguided attempts at the time of Congress' action to "sanitize" the eSign legislation of references to particular technologies – including PKI. This is much like fearing the inclusion in legislation of a specific description of appropriate practices for licensed air traffic controllers, because such regulations are silent on the licensing standards for barge operators.) Nonetheless, it is undisputed that if PKI, PKI-biometric hybrids or similar digital certificate-based authentication and encryption technology were in widespread use by eCommerce consumers, the risk of financial crime, identity theft and compromise of PII would virtually disappear for those using such tools. When these techniques are in use by a majority of eCommerce users, gain-seeking exploits will drop dramatically as a secure network becomes a less inviting target for bad actors.

2. Security Issues Relating to Consumers' Home Information Systems

* What steps can consumers take to reduce their security risks?
* What information resources or security products are available to help consumers protect themselves?

Many members of the information industry, including VeriSign, have joined with government agencies, including the FTC, to sponsor a new educational initiative, Stay Safe Online, http://www.staysafeonline.info/ , to bring precisely this awareness of techniques, tools and practical options before the eCommerce consumer.

* If consumers' lack of awareness or technical expertise lead to security vulnerabilities, what steps can be taken to raise awareness or educate consumers?
* What types of awareness and education initiatives are currently being pursued?
* What are the "best practices" being implemented by businesses to assist consumers in safeguarding their home information systems?

3. Security Issues for Businesses that Maintain Consumers' Personal Information

* What practical challenges do businesses face in securing their computer systems, and specifically consumers' personal information that is stored on them?
* What are the costs to businesses of security measures and of security failures?
* What measures can businesses, especially smaller businesses, take to secure their computer

systems and the consumer information stored on them? What information resources are available to help these businesses?

An excellent guide providing generic network security advice for business network operators and users (as well as detailed discussion of the previous two questions) is the Carnegie-Mellon University's Software Engineering Institute Computer Emergency Response Team's "The CERT Guide to System and Network Security Practices" by Julia H. Allen. This document is written with minimal technical jargon, is addressed to the non-engineer business network manager or business user of networks, and has information relevant to individual computer users, as well as direction to an abundance of primary source material. SEI/CERT utilizes this book in providing contract training in network security to business network managers.

* What are the "best practices" being implemented by businesses to address these issues?

As with the plethora of information sources that offer individual consumers advice about securing their own systems, an abundance of security practice recommendations exist for businesses, as well. Indeed, a number of the technology industry institutions have recognized the mixed blessing of such a vast amount of information, and are attempting to provide a catalogue of "best" or "effective" security practices – as opposed to 'one more best practices recommendation'. These have some generic common themes; however, sector-specific practices statements also exist. Indeed, even in individual sectors there are often competing collections of "best practices" statements, and one challenge is to identify appropriate security techniques for an individual enterprise, rather than relying on any one "canned" statement, or being locked into inaction because of a fear of selecting less-than-perfect guidance. Of particular interest is an effort by the Carnegie-Mellon CERT, with the aid of VeriSign and other Internet infrastructure technical experts, to develop a security engineering practices guide for Internet Service Providers, based on the CERT's widely praised OCTAVE practices guide. This effort is important because of the diversity of institutions functioning as "ISPs", and the lack of any common link to assure their maintenance of appropriate security hygiene measures, other than marketplace pressure imposed by the demands of their customers.

4. Emerging Business Models, Technologies, and Best Practices

* What are the existing business models for security, and are they sustainable over the long term?
* What technologies, business models, or initiatives are emerging in the marketplace to address the security of consumers' information?

(See answers to Question 1)

5. Revising the OECD Security Guidelines

Commissioner Orson Swindle is leading the U.S. delegation to the Organization for Economic Cooperation and Development ("OECD") Experts Group reviewing the OECD Guidelines for the Security of Information Systems. These voluntary guidelines contain principles which provide a

framework for participants to think about information and network security practices, policies, and procedures. The guidelines discuss cultivating a "culture of security" and contain nine policy principles for the security of information systems and networks, as well as principles relating to the life cycle of information systems and networks. The guidelines specifically address: raising awareness of security risks; responsibility for the security of information systems; designing security into system architecture; and risk management, assessment, and monitoring. Because the principles provide a helpful framework for thinking about security issues, the Commission plans to present a panel discussion on the Security Guidelines.

VeriSign has participated for over a year in industry working groups preparing comments for the OECD's Security Guideline revision exercise, and has participated in the advisory sessions Commissioner Swindle has graciously sponsored. The major continuing challenge in this exercise is the gap in cultural perspective between the United States and a number of the other OECD member nations, leading to a predilection towards highly granular and proscriptive regulations by individual states. In the highly competitive and rapidly evolving technological environment of the Internet, and, in particular, in the area of network security, the risk of overly-specific language remains of greatest concern. Freezing in place specific techniques or technologies (as contrasted with governmental recognition or approval of the appropriateness of deploying technologies), without providing for the capacity for their evolution in design and use is worse than not addressing the issue at all.

The United States and like-minded delegations participating in the OECD effort have a difficult responsibility in encouraging the OECD to recognize the continuing critical importance of security in our ever-increasingly security dependant information society, without making well-intentioned, but potentially damaging errors based on time-and-technology bound policies.

VeriSign, Inc.
By Michael A. Aisenberg
29 April 2002