United States Senate
Committee on Commerce, Science, and Transportation
Testimony of Paul B. Kurtz
Executive Director, Cyber Security Industry Alliance
May 10, 2005

Thank you Chairman Stevens and Co-Chairman Inouye for inviting the Cyber Security Industry Alliance (CSIA) to testify before this committee on Identity Theft/Data Broker Services. As Executive Director of CSIA, I am pleased to speak about the importance of securing personal identify information.

The Federal Trade Commission estimates that 27 million Americans were victims of some kind of ID theft in the past five years. Other studies suggest 1 in 20 U.S. citizens have been hit by electronic fraud. The numbers are staggering. Every electronic breach of personal information is another reason for consumers to lose trust in our information systems. A recent survey conducted by the Poneman institute revealed that 57 % of consumers with high trust in their primary bank say they would cease all online services with their current bank in the event of a single privacy breach. The loss of trust or confidence in our information systems inhibits economic growth, our security as citizens as well as a nation. CSIA believes the right approach to securing consumers' personal data requires a blend of appropriate policies, technical expertise and security technologies.

A central question before this Committee today is defining the government's role—whether directly or indirectly—in protecting personal information residing on information systems owned and operated by the private sector. This Committee, rightfully, will also look at where the marketplace is succeeding at protecting personal information and where it is failing. At this critical time of technology development and innovation, the United States, as an economic force and a global technology leader, must carefully chart a public policy approach to information security that continues to encourage innovation while also providing protections.

In my testimony today, I will cover four areas.

- A brief introduction to CSIA;
- Security challenges in securing electronic data;
- Solutions and market activity;
- Recommendations for Congress' consideration in securing electronic data.

Introduction to CSIA

CSIA is dedicated to enhancing cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. CSIA is led by CEOs from the world's top security providers, who offer the technical expertise, depth and focus to encourage a better understanding of cyber security policy issues. We believe that ensuring the security, integrity and availability of global information systems is fundamental to economic and national security. We are committed to working with the public sector to research, create and implement effective agendas related to national and international compliance, privacy, cybercrime, and economic and national security. We work closely with other associations representing vendors, critical infrastructure owners and operators, as well as consumers.

CSIA's initiatives range from examining the cyber security implications of Sarbanes-Oxley to the security and reliability of Internet telephony, also known as Voice over IP, to advocating more government leadership in identifying and protecting critical information infrastructure.

CSIA understands that the private sector bears a significant burden for improving cyber security. CSIA embraces the concept of sharing that responsibility between information technology suppliers and operators to improve cyber security. Cyber security also requires bi-partisan government leadership.

Members of the CSIA include BindView Corp; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc.; iPass Inc.; Juniper Networks, Inc.; McAfee, Inc; PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation; Symantec Corporation and TechGuard Security, LLC.

Challenges in Securing Electronic Data

Many large organizations, from corporations to universities and health care systems, are conducting more of their business using network technology such as the Internet. Therefore, customers, employees, students and patients are having their personally identifiable information gathered into vast electronic data storage repositories. Some industries already have requirements to protect personally identifiable information, such as the banking and health communities. Laws and regulations are being created at various levels to address security and privacy because the criminal activity related to stealing these electronic data is increasing exponentially. Multiple laws requiring potentially different requirements will quickly make compliance an overly complex task.

The problem of ensuring security and confidentiality of electronic data is complex. There are two fundamental areas requiring protection. The first is ***protecting the storage*** of personal information in data warehouses such as names, addresses and Social Security

numbers. The second is ***protecting the movement*** of these data to and from the data warehouse.

Technical security safeguards are used to address both the storage and movement issues. Policy is also crucial for it governs implementation of the technical safeguards and access to the data. Movement of the data amplifies the challenge of security because it creates weak points in the system. Those points are often *outside* the direct control of security administrators overseeing data warehouses. The movement of data makes it difficult to define the set of users who should take action to ensure the security of personal information by a select group. Therefore, policy and best practices play a pivotal role in shoring up weak points.

The core information technology application of large data holders is a "data warehouse." It accumulates disparate records then analyzes, stores and distributes a vast amalgamation of information – billions of records about hundreds of millions of Americans. Many elements of the technology require special provisioning for security, including applications, systems and networks. A secure solution requires security provisions at the original source of data, at the data holder, at service providers, and at each customer location accessing the warehouse. The holder's control of security diminishes as information passes over external networks. Control vanishes once information is injected into the customer's internal applications.

The data warehouse's database management system handles security and access control. Securing the warehouse is mostly a function of establishing, granting and updating access control permissions and rights – a configuration process based on policy. Security requirements extend to appropriate configuration of access controls and permissions for software applications feeding information into the data warehouse.

Data warehouse technology operates on a networked system of servers. The servers may physically exist on premise at the data holder or at an external hosting service provider. Other systems for the data warehouse include access devices such as PCs, laptops, handheld computing devices, and telephones. Primary security for all systems is mostly a function of their operating systems. Proper installation, configuration and patching of bugs in the operating system software are crucial for secure systems.

Solutions and Market Activity

Before considering steps the government should take to facilitate securing electronic data, it is appropriate to discuss solutions and market activity. There is no "silver bullet" technical or policy solution to secure data warehouses. A variety of technologies and policies are required. Key technologies and policies include:

- **Policy Management**: Enforces security rules and regulations. Provides guidance to management on who should access what, when and where

- **Vulnerability Management**: Remediate vulnerabilities through scanning devices that identify and patch vulnerabilities, as well mitigate misconfigurations, unnecessary services, unsecured accounts, and malicious code. Addressing major classes of network and desktop vulnerability improves IT enterprise and operational stability.

- **Intrusion Detection/Prevention**: Technologies that monitor content of network traffic for infections and block traffic carrying infected files or programs. Reducing incoming sick traffic closes another window for criminals to access these data

- **Authentication**: A critical first step to ensuring only appropriate users may access the data is using digital certificates and multiple factor authentication. This is a way to confirm legitimate customers and control internal end user access. Strong authentication also mitigates the problem of passwords, which are inherently weak, from being hacked or otherwise compromised.

- **Access Controls**: Ensure that authenticated users and applications can access only that data and information which they have been granted authority to use. Access controls may be based on a number of factors, including an individual's role in an organization. They are particularly important to prevent insider attacks and as a deterrent to inappropriate browsing of sensitive data.

- **Audit Files**: Detailed and protected records of computer and network traffic and transactions that can help ensure policy compliance and assist in forensic investigations of computer crime.

- **Encryption**: Transforms data into password (key)-protected packets that prevent reading by unauthorized users. Secure communication enables data warehouse vendors to safely and efficiently serve their customers.

- **Anti-Virus**: Software automatically checks new files for infection. Inoculates PCs and applications from diseased software code attempting to cause harm.

- **Firewall**: Blocks unauthorized traffic from entering PCs and servers from the Internet. Protects end users from unwanted activity on their PCs.

Some enterprises are beginning to see security as a means to differentiate themselves from their competition. For example, a well known e-trading firm is working with a CSIA member to use two factor authentication to improve the security of customer accounts. Some Internet Service Providers (ISPs) are differentiating themselves from others by highlighting the steps they are taking to protect personal information. Other CSIA member firms are providing managed security services, encryption technologies, intrusion prevention, vulnerability management services to a variety of owners and operators of infrastructure.

Policy Considerations for Securing Electronic Data

The security of data warehouses will require a blend of appropriate policies, technical expertise, and security technologies. Technical provisions for security are aimed to thwart unauthorized access to personally identifiable information – whether by electronic hackers who break in by securing a legitimate password (e.g. NexisLexis), or by in-person fraud (e.g. ChoicePoint). Technical provisions are only as strong as the security policy which implements them.

Security breaches of data warehouses can adversely affect the life of any American so it is appropriate for Congress to establish national policies in conjunction with the private sector for the protection and privacy of personal information.

While Congress is largely focused on data brokers, the protection of personal information is also critical in other businesses where data warehouse technology is used and where similar risks exist. Congress should examine the issue more broadly as it contemplates the need for legislation.

In this context, CSIA recommends Congress to consider the following:

- Take a holistic approach to addressing cyber security. Currently, Congress is considering cyber security problems such as spyware, phishing, and data warehouse security on an individual basis. In fact, each of these problems has at least one issue in common: the attacker is seeking and individual's personal information in order to commit financial fraud. We can anticipate similar exploits in the future.

- Harmonize any new legislation with existing legislation at the federal level, filling gaps rather than duplicating requirements already contained in existing law, such as Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accounting Act (HIPAA) and the Fair Credit Reporting Act (FCRA). Use existing security standards wherever possible, rather than creating new ones. This approach would provide a framework for identifying areas of risk, as well as encouraging industry best practices.

- A piecemeal approach by Congress, in conjunction with the numerous laws states are passing will present consumers and businesses with a "patch work" quilt of confusing laws and complicated compliance issues**.** Already states are stepping into the void and creating a confusing patchwork of legislation on the issue. Legislation regulating Spyware has been introduced in 24 state legislatures this year, with approaches ranging from studies to changes in criminal code. Anti-phishing legislation is sitting on the Governor's desk in Hawaii, and pending in states including Texas and Florida. And there are more than 300 bills pending on identity theft in our nation's state legislatures. A federal preemption of the many laws recently passed or currently contemplated at the state level related to spyware, phishing, and data broker security would alleviate much of the concern

and consternation within the private sector as a whole. However, any preemptive federal law should maintain, at the minimum, the security standards already put in place by corresponding state legislation.

- Encourage broader use of security technologies *without* mandating specific technology solutions. Urge adoption of the approach utilized in CA 1386 which calls for disclosure of a breach involving unencrypted data.

- To encourage stronger cyber security, Congress should investigate incentives, including "safe harbors", tax benefits, 3rd party or self certification, insurance and the adoption of best practices, *without* mandating specific technology solutions. Dictating a specific technology is counter-productive as it stifles innovation and discourages creativity.

- Congress should increase penalties for identity theft and other cyber crimes as well as ensure appropriate resources are available to law enforcement authorities. The Senate should swiftly ratify the Council of Europe's Convention on Cybercrime which would create a global framework for investigating and prosecuting cyber criminals.

- Congress should also take a long-term view of information security. There is no coherent cyber security R&D agenda. Significant Federal funding is closeted in classified programs. While our national security needs must be met, we must anticipate that privately owned and operated networks will be attacked as well. We need to develop resilient, fault tolerant networks which degrade gracefully under attack.

Leadership in information technology is a constantly moving target. As the technology changes and improves, so must its security. Likewise, as the need for public protection evolves, so must our public policy. We call on Congress and the Administration to work with the private sector to develop a holistic approach to protection our nation's personal information.