



2020 14TH STREET
SUITE 750
ARLINGTON, VA 22201
TEL: 202-204-0838
WWW.CSIALLIANCE.ORG

August 1, 2005

Lisa Wallmeyer
Director
Joint Commission on Technology and Science
910 Capitol Street, Second Floor
Richmond, VA 23219-0406

Dear Ms. Wallmeyer:

On behalf of the Cyber Security Industry Alliance (CSIA) I am pleased to submit comments on the proposed House Bill no. 2721. Led by CEOs from the world's top security providers, CSIA is the only advocacy group dedicated exclusively to enhancing cyber security through public policy, education, awareness and technology. We offer technical expertise, depth and focus to encourage a better understanding of cyber security issues.

We appreciate the efforts of the Joint Commission on Technology and Science as well as those of the Virginia General Assembly to address the problem of security breaches relating to personally identifiable information. Below we have included a number of principles that we have shared with federal legislators in their efforts to draft a national statute.

In the interest of transparency it should be made clear that CSIA favors federal preemption with regard to data security and data breach notification. Without preemption, those entities that hold sensitive personal information may be subject to fifty different, and possibly conflicting, standards as to who must be notified, when they must be notified, and how notification must take place. Such a potentially complex regulatory web will quickly overly burden local and national business interests. For example a Virginia business would potentially be required to develop up to fifty different response policies in order to deal with a single breach of their data security. Developing adequate responses would be prohibitively expensive. Despite CISA's preference for a national standard we believe that state Attorney Generals should have to ability to protect their citizens' rights and sue unscrupulous entities that do not maintain proper security in state and federal courts under the federal statute.

Within the context of CSIA's position we offer the following five key principles that we have previously shared with members of Congress as they drafted legislation touching on this issue. We realize that each principle may not correspond directly with your needs but we wanted you to have the same document given to Congress. We invite you to review these principles as you work on a HB 2721 and future legislation:

1. Federal Pre-emption. Any new law should establish a national data breach notification “floor” for unauthorized access to unencrypted personal information while enabling state attorney generals to prosecute the Federal law so long as the U.S. Attorney General is notified.

2. Scope. The scope of a breach notification bill should apply to any agency or person, as defined in title 5 of the U.S. Code, who owns or licenses computerized data containing sensitive personal information and should not be limited to data brokers.

Legislation should address “gaps” in existing legislation related to the security of personal information. Recent security breaches have occurred in a variety of organizations, ranging from data brokers, banks and hospitals, to educational institutions and large employers.

3. Reasonable Security Practices. Reasonable security practices encompass a combination of technology, policy, and expertise. Consistent with existing State law, organizations that own or license computerized data containing personal information should implement and maintain reasonable security measures based on widely accepted voluntary industry standards or existing Federal law.

Security Practices. The term ‘security practices’ shall mean reasonable security and notification procedures and practices appropriate to the nature of the information to protect sensitive personal information from unauthorized access, destruction, use, modification or disclosure.

Certification. Legislators could consider self-certification to help safeguard sensitive personal information. In the case of self-certification, covered entities would be required to self certify that they have met a widely adopted standard in order to safeguard sensitive personal information. If a breach occurs and it is clear that reasonable measures were not taken to safeguard sensitive personal information, then the covered entity involved would be subject to criminal prosecution. Legislators could also consider an option for certification by a 3rd party coupled with liability protection to foster protection.

Encryption. Legislators should encourage the use of encryption technologies without requiring it, similar to California's SB 1386. (We appreciate that HB 2721 already includes such a provision regarding encryption). Encryption is defined as “The protection of data in storage or in transit using an encryption algorithm implemented within a validated cryptographic module that has been

approved by NIST or another recognized standards body, combined with the appropriate key management mechanism to protect the confidentiality and integrity of associated cryptographic keys in storage or in transit.”

Existing voluntary standards include:

International Standards Organization (ISO) 17799
Control Objectives for Information and Related Technology (COBIT)
British Standard (BS) 7799
Information security governance framework issued by the National Cyber Security Summit Task Force in April 2004

Existing regulatory standards include:

Fair Credit Reporting Act (<http://www.ftc.gov/os/statutes/fcra.htm#607>)
Gramm Leach Bliley, Safeguards Rule
FDA, Title 21, Subchapter A, Protection of Privacy
Basel II, Revised International Capital Framework
Health Insurance Portability and Accounting Act (HIPAA) Security Rule

4. Definition of “breach.” A breach of unencrypted personal information should be defined so that it encourages the implementation of reasonable security measures and minimizes false positives.

5. Regulatory Authority. The Federal Trade Commission is the most appropriate authority to oversee breach notification on a civil level and refer criminal cases to the Department of Justice. Wherever possible, the FTC should be directed to adopt existing standards, rather than to create new standards.

We hope these principles are helpful to both the Joint Commission on Technology and Science as well as to the larger General Assembly. The issue of notification for security breaches of databases containing personal information is important.

If you have any further questions or believe CSIA or any of our member firms may be of further assistance please don't hesitate to contact my office.

Best Regards,

A handwritten signature in black ink, appearing to read "Paul B. Kurtz". The signature is stylized with a large, sweeping flourish at the end.

Paul B. Kurtz
Executive Director