LATE

NEIL ABERCROMBIE
GOVERNOR

BRUCE A. COPPA
Comptroller

RYAN OKAHARA
Deputy Comptroller

STATE OF HAWAII
DEPARTMENT OF ACCOUNTING
AND GENERAL SERVICES
P.O. BOX 119
HONOLULU, HAWAII 96810-0119

TESTIMONY
OF
BRUCE A. COPPA, COMPTROLLER
DEPARTMENT OF ACCOUNTING AND GENERAL SERVICES
TO THE
SENATE COMMITTEE
ON
ECONOMIC DEVELOPMENT AND TECHNOLOGY
AND
JUDICIARY AND LABOR
ON
January 31, 2011

S.B. 1162

RELATING TO SECURITY BREACHES OF PERSONAL INFORMATION

Chair Fukunaga, Chair Hee, and members of the Committees, thank you for the opportunity to testify on S.B. 1162.

While the Department of Accounting and General Services does support the overall intent of SB 1162, we are unable to support this bill without clarification on several points.

First, we believe equal provisions should apply to incidents that occur in both the public and private sectors. It is clear from the public record that no sector is immune from data security issues, and the next breach could as easily be from an insurance company, healthcare provider or private college as another UH campus or state or county agency.

Second, providing remedy for individuals impacted by data breaches is clearly the responsibility of the party that incurred the breach whether public or private. Damages in a cyber liability case have been left to the courts to determine and may be addressed by risk management. Let me go into more detail on this point.

Mandatory credit reporting requirements will increase the cost of government and business in Hawaii. Mandatory credit reporting requirements generally notify individuals after-the-fact. Although early notification can be helpful, this is less effective than stopping the crime

via enhanced training before breaches occur or technical solutions that eliminate the need for use or retention of personal information. Focusing on credit monitoring services for those impacted by a data breach provides protection for only a small set of victims of identity theft since most identity theft does not result from data breaches. An alternative approach would be to provide improved protection against ID theft such as requiring credit agencies to provide free and convenient credit freeze services to anyone who is notified of a data breach by any public or private organization. This would help prevent identity theft rather than help detect it after-the-fact. And unlike the current legislation, it would protect Hawaii residents who are notified of breaches by national organizations as well, including the federal government, credit card companies, alumni associations, hotels and online merchants. Further extension of free credit freeze services to all Hawaii residents, whether or not they have been notified of a breach, would even more strongly protect Hawaii citizens from identity theft, most of which has origins other than local data breaches. This approach would have no additional direct costs to Hawaii businesses or government and would provide significantly greater protection to consumers beyond those who might be affected by local public or private sector data breaches.

While credit monitoring or credit freeze services may be a legitimate remedy, the administrative, logistic and monetary cost to an entity (private or public) to provide credit report services to every possible breach notification could be staggering. For public agencies to provide commercial credit monitoring services in a timely manner, either a master contract would need to be in place or the selection of the service would need to be fully exempt from HRS103D. Otherwise it would be a months-long process to develop specifications and conduct a successful competitive solicitation to choose among private for-profit vendors.

Enrolling in a credit monitoring service requires provision of a full complement of personal indentifying information (PII), including the SSN. This should be performed directly between the individual and the credit monitoring vendor. It would much less secure and more time-consuming to involve the entity that performed the notification into the mechanics of providing the individual's PII to the credit monitoring vendor and executing the enrollment.

Third and finally, we feel the bill does not address funding for the specific resources necessary to implement this Bill and our specific requirements follow:

Additional Recommendations

In reviewing the bill provided, we have some specific comments relative to awareness, training, staffing and technology.

1. We would expect ICSD, as the experts in Cyber-Security topics, to develop awareness of what should be done, risks involved, and understanding of consequences for non-compliance. We would not expect each agency to develop their own training. We envision a base level curriculum made up of computer based training that agencies can use "as is", and either tailor to their specific circumstances or supplement with agency specific hands-on training. Once the base modules are developed they could be turned over to DHRD to manage, coordinate enrollment, and track attendance to report back to the IPSC regarding compliance. At least annually, ICSD would review the curriculum and create updates as needed.

2. Relieve individual departments from having to be experts in security training, tools, regulations, basic laws, and policies that apply to agencies statewide. Let them trust that ICSD will do that and let them know if they are out of synch. Agencies can then concentrate on privacy and security issues specific to their agency. (e.g. Hippa etc.)

3. A study should be commissioned to examine where State systems or processes utilize SSN numbers when not required by federal or other mandate. Determine if an employee number or other identifying number could be used, and determine the costs and staffing needs to update these systems.

Staffing Requirements

To properly carry out the spirit of this bill, it is felt that the staffing that was not included in the original Act 10 be properly addressed.

The bare minimum staff and what their duties could consist of include:

- Statewide Security Scanning Coordinator (1)
  Provide real Time ongoing scanning as the ICSD does today, but extended and expanded statewide and include features ICSD currently does not have such as SSN filters, TripWire type tools for change detection, Websense for traffic monitoring, etc.

- Statewide Network Security Coordinator (1)
  Provide analysis of Firewall placement and rule sets. Establishes general enforceable guidelines for all firewall definitions statewide. Authority to scan across and through firewalls to check for exposure to inadvertent penetration. Responsible for coordination of an annual external security audit (could be federal or private), and report to IPSC of findings and the required management response for corrective action similar to the current ICSD SAS/70 audits but at the network level. If the State used managed services in selected areas, this position would be the managed services watchdog.

- Statewide Application Scanning Service Specialist (1)
  Provide departments and agencies with ongoing active scanning, and reports on their applications that may expose any programming faults that have the potential to provide hackers with access to confidential information. Findings would be tracked and reported to the IPSC, and provide the required management response for corrective action. Provide annual application audit for selected public facing applications.

- Security Incident Specialist (1)
  Breaches will be coordinated through ICSD for awareness, understanding, and documentation. The breach expert will facilitate the inclusion of appropriate legal, law enforcement, public information officer, and compliance entities. This would include the use of standardized reporting templates and communication models.

- Training Coordinator(1)
  A training coordinator directly addresses the draft legislation. Self directed learning may create familiarity with policies, best practices and guidelines but may not always surface

the risks that exist the way individual education can. It needs to be ensured that DHRD is on board, able, and willing to assist as this would be a statewide training effort that requires accountability.

- Clerical/Administrative Support (1)
  Provide IPSC support for the necessary added reporting, scheduling, and follow-up required to facilitate the knowledge the IPSC needs for training, data scanning, network security, application scanning compliance, incident coordination, and reporting.

ESTIMATED GENERAL FUND STAFF COSTS: 5 * 70,000 = $350,000 annual operating. The staff be housed as part of the ICSD Cyber Security Team and provides reports to IPSC.

Security Tools, Maintenance & Licenses

The State does not own sufficient modern automated tools that can automate the detection of security or breach issues. Doing so by hand, given the breadth of systems that the State maintains, is not technically feasible. Below is a recommendation of the minimum amount of tools required to provide a basic level of protection and detection. It is highly recommended to ensure that the State receives the maximum vendor discounts that these items be procured on a statewide basis and not agency by agency, and that State procurement modifications are made to allow us to take advantage of established Federal DOD programs and discount levels.

- Statewide change management software to detect unauthorized changes in cyber security systems, systems containing PII, application code, and configuration files.
- Expansion of existing web application scanning software (ATG and ICSD have some basic software already).
- Expansion of active security monitoring software.
- Mandatory managed anti-virus for all State owned servers, desktops, and laptops.
- Mandatory disk encryption for laptops that contain PII.
- Mandatory anti-spam / anti-virus scanning for all e-mailboxes.
- Estimated cost for the above: $875,000 initially for acquisition, with $170,000 annual operating costs. Note that existing staffing levels could not feasibly implement and manage these new tools.

Total General Funds Required:	Initial Yr	Recurring/Annual
Staffing:	$350,000	$350,000
Security Tools/Maintenance/Licences:	$875,000	$170,000
Total:	$1,225,000	$520,000

Thank you for the opportunity to testify on this matter.