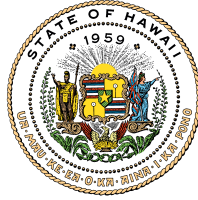


NEIL ABERCROMBIE
GOVERNOR



STATE OF HAWAII
OFFICE OF INFORMATION MANAGEMENT & TECHNOLOGY

P.O. BOX 119, HONOLULU, HAWAII 96810-0119
www.hawaii.gov/oimt

**SANJEEV "SONNY"
BHAGOWALIA**
CHIEF INFORMATION
OFFICER

RANDY BALDEMOR
DEPUTY CHIEF INFORMATION
OFFICER – BUSINESS
TRANSFORMATION

KEONE KALI
DEPUTY CHIEF INFORMATION
OFFICER – OPERATIONS

TESTIMONY OF
SANJEEV "SONNY" BHAGOWALIA, CHIEF INFORMATION OFFICER
TO THE HOUSE COMMITTEE ON
ECONOMIC DEVELOPMENT AND BUSINESS

Friday, March 15, 2013

9:00 a.m.

Hawaii State Capitol Conference Room 312

S.B. 1003, S.D. 2

RELATING TO INFORMATION TECHNOLOGY

Chair Tsuji, Vice Chair Ward and members of the committee, thank you for the opportunity to testify on S.B.1003, S.D. 2.

The Office of Information Management and Technology (OIMT) strongly supports S.B. 1003, H.D. 2 and urges the committee to pass this measure.

As you may have read in the February 2, 2013 edition of the Honolulu Star-Advertiser, the State of Hawaii's computer systems are indeed targets of hackers, cyber-thieves, and cyber-terrorists. In today's digital age, information is a highly valued commodity and one that must be protected from external and internal threats.

Thus, safeguarding the State's information and data is of vital importance. The Office of Information Management and Technology (OIMT) has developed a comprehensive Business and Information Technology/Information Resource Management (IT/IRM) Transformation Plan and one of the top ten initiatives outlined is Security and Privacy. Under the plan we will provide a singular enterprise vision for information assurance and data protection, unify cyber security and information assurance practices across the state and put into place best practices.

Cyber security threats are a persistent and growing concern as the continued advances in and increasing dependency on the information technology permeates our modern society. It is also of economic concern, as breaches are measured in the tens of millions of dollars and potential loss of public trust.

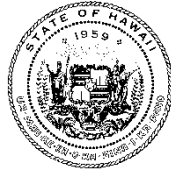
The extent of the challenge is laid out in the Transformation Plan and includes a detailed solution to address the problems. OIMT has also recently completed a security assessment that provides a benchmark against all states and their standards, more details on the 17 areas that need to be addressed, and identifies 48 projects ameliorate our current gaps. The State must improve its current cyber security, as they are ineffective and inadequate to meet the increasingly sophisticated threats.

We have begun to address the problems through pilot projects, but it will take much more investment to prevent hackers, cyber-thieves and cyber terrorists from accessing the State's information assets. Our plan calls for consolidating systems, which will enable us to implement unified standards and processes across the departments and have a dedicated team of trained IT professionals monitoring and addressing cyber security issues. This centralized security will be enhanced with collaborative surveillance and joint enforcement. Most importantly, security must be built-in throughout the entire information management process – from creation to transmittal to storage.

While even the most sophisticated security devices can protect against cyber threats and attacks, the most important component is trained, experienced personnel to proactively prevent and react when these threats occur. The State not only needs to improve its procedures, policies and technology, but also remove “it can't or won't happen here” mentality.

S.B. 1003, S.D. 2 provides the statutory authority for the Chief Information Officer to execute the Security and Privacy Plan including establishing and implementing standards and defining the scope and regularity of security audits, which will enable the State to continuously improve its cyber-security posture.

We respectfully request that this Committee move this bill forward. Thank you for the opportunity to testify on this matter.



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

TESTIMONY
OF
DEAN H. SEKI, COMPTROLLER
DEPARTMENT OF ACCOUNTING AND GENERAL SERVICES
TO THE
HOUSE COMMITTEE
ON
ECONOMIC DEVELOPMENT & BUSINESS
ON
March 15, 2013

S.B. 1003, S.D. 2

RELATING TO INFORMATION TECHNOLOGY

Chair Tsuji and members of the Committee, thank you for the opportunity to testify on S.B. 1003, S.D. 2.

The Department of Accounting and General Services strongly supports S.B. 1003, S.D. 2, an administration-sponsored measure.

By granting authority to the State chief information officer to protect and secure the State of Hawaii's information and data communication infrastructure, this bill will support and enhance existing cyber security activities that the Information and Communication Services Division has developed and implemented. For the Committee's information, section 487N-5, Hawaii Revised Statutes, established the information privacy and security council, whose scope includes initiatives to mitigate the negative impacts of identity theft incidents on individuals and the measures all parties (including government) should take to safeguard their systems from

intrusions and loss of confidential information.

Thank you for the opportunity to testify on this matter.

NEIL ABERCROMBIE
GOVERNOR



BARBARA A. KRIEG
DIRECTOR

LEILA A. KAGAWA
DEPUTY DIRECTOR

STATE OF HAWAII
DEPARTMENT OF HUMAN RESOURCES DEVELOPMENT
235 S. BERETANIA STREET
HONOLULU, HAWAII 96813-2437

March 13, 2013

TESTIMONY TO THE
HOUSE COMMITTEE ON ECONOMIC DEVELOPMENT AND BUSINESS

For Hearing on Friday, March 15, 2013
9:00 am., Conference Room 312

BY

BARBARA A. KRIEG
DIRECTOR

Senate Bill No. 1003 Senate Draft 2

RELATING TO INFORMATION TECHNOLOGY

WRITTEN TESTIMONY ONLY

TO CHAIRPERSON TSUJI AND MEMBERS OF THE COMMITTEE:

The purpose of S.B. No. 1003 S.D. 2 is to allow the Chief Information Officer (CIO) the ability to establish policies and procedures and standards to regularly assess security risks, determine appropriate security measures, and perform security audits of government information systems and data communications infrastructures across all departments, agencies, boards, or commissions.

The Department of Human Resources Development (DHRD) strongly supports this bill.

DHRD is responsible for ensuring that all employee information and data within the Human Resources Management System (HRMS) is maintained in a secure environment for authorized personnel specialists within all departments of the State Executive Branch, not including the Department of Education and the University of Hawaii. Furthermore, the department is responsible for conducting all the recruitment and screening of applicant data for individuals seeking potential employment with the State.

Although the department has implemented measures to ensure that the appropriate security measures are in place, it does not have sufficient resources to implement updated technology and infrastructure that may be required to detect new security threats or risks.

Therefore, we support the proposed amendments to the bill and thank you for the opportunity to provide testimony in strong support of S.B. 1003 S.D. 2.