LATE

NEIL ABERCROMBIE
GOVERNOR

STATE OF HAWAIʻI
OFFICE OF INFORMATION MANAGEMENT & TECHNOLOGY
P.O. BOX 119, HONOLULU, HAWAIʻI 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 SENATE COMMITTEE ON
WAYS AND MEANS
Thursday, February 21, 2013
9:00 a.m.
Hawaii State Capitol Conference Room 211

WRITTEN TESTIMONY ONLY
S.B. 1003, S.D. 1

RELATING TO INFORMATION TECHNOLOGY

Chair Ige, Vice Chair Kidani and members of the committee, thank you for the opportunity to testify on S.B.1003, S.D. 1.

The Office of Information Management and Technology (OIMT) strongly supports S.B. 1003, H.D. 1 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 the 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 more details on the areas that need to be addressed. 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 no 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. 1 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.