

NEIL ABERCROMBIE
GOVERNOR



LATE TESTIMONY

BANJEEV "BOB" BHAGDWALIA
CHIEF INFORMATION OFFICER

RANDY BALDENOR
DEPUTY CHIEF INFORMATION OFFICER - BUSINESS TRANSFORMATION

KEONE KALI
DEPUTY CHIEF INFORMATION OFFICER - OPERATIONS

STATE OF HAWAII
OFFICE OF INFORMATION MANAGEMENT AND TECHNOLOGY
P.O. BOX 119, HONOLULU, HAWAII 96810-0119
www.hawaii.gov/oimt

TESTIMONY OF
KEONE KALI, DEPUTY CHIEF INFORMATION OFFICER
TO THE SENATE COMMITTEE ON PUBLIC SAFETY, INTERGOVERNMENTAL AND
MILITARY AFFAIRS, AND SENATE COMMITTEE ON TECHNOLOGY AND THE ARTS

Thursday, February 6, 2014
1:45 p.m.
Conference Room 414
State Capitol

S.B. 2474
RELATING TO CYBERSECURITY

Chair Espero, Chair Wakai, Vice Chair Baker, Vice Chair Nishihara, Members of the Committees:

I am Keone Kali, Deputy Chief Information Officer (Operations), in the State Office of Information Management and Technology (OIMT), speaking in support of the intent of S.B. 2474 to improve the State's cybersecurity.

In today's global digital world, cyber security threats are a persistent and growing concern as we increasingly depend on information technology for our daily activities. The rising number of data breaches continues to produce significant financial losses and economic consequences, as reflected by recent data thefts from Target and Neiman Marcus that affected tens of millions of customers.

The OIMT has statutory responsibilities to protect government information and data communication infrastructure from unauthorized uses, intrusions, and other security threats. To carry out those responsibilities, OIMT is working with state departments and agencies to implement State government's Security and Privacy Plan that includes establishing cyber security standards, unifying cyber security and information practices, on-going security audits, and embracing industry best practices for cyber education and training.

Similarly, the State Department of Defense works closely with public and private sector operators to protect the State's critical infrastructure from natural and man-made threats. We defer to the Department of Defense to best coordinate cyber resiliency programs among its critical infrastructure partners. We agree that increasing cyber security collaboration within that group and others in the community will greatly improve the State's cyber security posture. OIMT will actively support DOD's community-wide cyber efforts by sharing staff and best practices from government's cyber programs.

We thank the committee for this opportunity to testify in support of reducing the State's cyber risks.