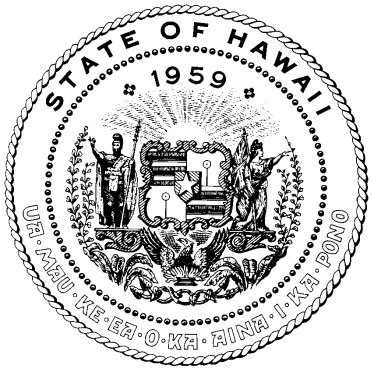

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

QUARTERLY REPORT ON

PERIODIC INFORMATION SECURITY AND PENETRATION AUDITS OF THE EXECUTIVE BRANCH INFORMATION TECHNOLOGY SYSTEMS

APRIL 1, 2016

SUBMITTED TO

THE TWENTY-EIGHTH STATE LEGISLATURE

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES
STATE OF HAWAIʻI

Quarterly Report on Periodic Information Security and Penetration Audits
of the Executive Branch Information Technology Systems
April 1, 2016

The Office of Enterprise Technology Services (ETS) submits this fourth report regarding periodic information security and penetration audits of the Executive Branch information technology systems, pursuant to Section 42-5 of Act 119, Session Laws of Hawaiʻi (SLH) 2015.

Should legislators require additional details, ETS is available upon request to provide a secure briefing.

Background

Cybersecurity authorities and responsibilities within State of Hawaiʻi government are outlined in statute as follows:

HRS §27-43	Establishes the CIO function
HRS §27-43.5	Provides cybersecurity authority to state CIO
HRS §487N	Requires departments to prepare security and information protection plans
HRS §487R	Reporting requirements for government agencies in case of breach

Security remains a high priority in the Internet age, as the threat has expanded from the lone hacker in a high school classroom, to state- and nation-sponsored cyber terrorism. Government agencies are a primary target for the cyber terrorist, whose attacks are becoming more and more sophisticated. The State currently has millions of attempted attacks each day with the bulk of them being thwarted.

Approach to Cybersecurity

Shortly after stepping into the role of State Chief Information Officer (CIO) in May 2015, Todd Nacapuy identified cybersecurity as one of six "CIO priorities" (workforce development, IT governance, services-oriented infrastructure, enterprise programs & projects, open government, and cybersecurity). Over the past year, much progress has been made to improve cybersecurity around State information technology systems and infrastructure.

Approximately 30-40 million intrusion attempts are blocked daily. Of the remaining traffic, ETS investigates an average of four suspicious items per day, ranging from malware, to denial-of-service attempts, to peer-to-peer attacks.

ETS' approach to cybersecurity includes network topology, technology and software tools, continuous monitoring and information sharing, response to threats and recent incidents, and awareness and education. It is not a one-size-fits-all approach, but rather requires flexibility in the face of different threats, vulnerabilities and risk tolerances, and includes various countermeasures.

As previously reported, ETS is working with the U.S. Department of Homeland Security (DHS) and FBI to take advantage of Federal resources and expertise, including DHS' Hygiene Program. ETS is also building staff and security tools capacity for alerting and/or corrective and proactive action spanning tens of thousands of desktops and servers.

Defense Requires "Lean-Forward" Technology and Process:

- Federally funded Managed Security Services from Center for Internet Security (CIS) / Multi-State Information Sharing & Analysis Center (MS-ISAC) monitor and respond to threats and attacks on network, 365/7/24. Security events spanning thousands of desktops and servers are analyzed and correlated for alerting and/or action.
- Local Enterprise Security Information and Event Management (SIEM) system collects and analyses thousands of security events and logs from internal monitoring points.
- Data Loss Prevention (DLP) protects against data leakage key capability to support State privacy protection efforts, e.g., social security numbers and personally identifiable information (PII).
- Alerts and notices are transmitted to Data Processing (DP) Coordinators and IT Governance Technical Committee members, for remedial action and to use in security awareness programs.

**Note: State staffing limitations currently confine service to an 8 a.m. to 5 p.m. schedule.*

Recent Progress

Office 365 Helps Address End-Point Security

Shortly after becoming CIO, Todd Nacapuy announced a significant acceleration for the State's Office 365 project, from a previous two-year implementation schedule.

The project scope includes most Executive Branch departments, excluding the Department of Education and University of Hawai'i. Benefits include fortified security and greater disaster recovery capability, in addition to expanded applications and services, added tools for collaboration, and long-term budget sustainability. (Product support for Lotus Notes, which the majority of State workers had been using for email under various agreements, ended last year on June 30 for those agencies under ETS' scope, with limited best-effort support provided, if necessary, to ensure business continuity.)

In May 2015, approximately 3,000 user licenses had been deployed. Since then, ETS has worked with departments to successfully deploy an additional 8,600+ user licenses — totaling more than 11,600 to-date — along with the many tools and enhanced resources now available to state personnel.

Deployment of any remaining licenses is pending department timetables. For example, the Department of Taxation, which recently launched its Tax System Modernization project, has opted for a limited deployment at this time in part to accommodate the modernization initiative as well as annual tax deadlines.

ETS and UH Data Center Colocation Agreement Provides Resilient Backup
A memorandum of agreement (MOA) between ETS and the University of Hawai‘i Information Technology Services (ITS) signed on March 15, 2016, leverages the UH IT Center to reduce risks associated with some of the State's IT systems while saving taxpayer dollars. The MOA specifies the terms of the colocation agreement under which some of the IT systems currently housed at that State's primary data center in the downtown Kalanimoku Building are migrating to UH's LEED Gold-certified data center to the extent possible to provide resilient backup.

The agreement also outlines a rate structure under which ETS will remunerate the university for its costs each year, including a "true up" based on actual expenses from the previous year.

The Kalanimoku data center has long been known as an aging facility with many components requiring refurbishment and upgrades. The Executive Branch and UH teams worked together on this mutually beneficial and cost-effective solution to meet our state's immediate data center needs. By leveraging the UH data center, the State is able to address some of its most critical systems while reducing duplicative spending, including costs associated with designing, building, maintaining, powering and staffing an entirely new data center.

Physical security, access and reliability were key factors in identifying the UH IT Center as a viable site. The UH facility already maintains a secure environment with protocols in place for authorized personnel are provided access, and the UH IT Center's data center is designed to operate through an extended power outage without any problems. In addition, under the MOA, the university agrees to put in place processes and procedures necessary for some state departments' compliance obligations, such as those required by the Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service, U.S. Department of Justice, and State and Federal personally identifiable information (PII) standards.

Further Improving Cybersecurity
Several key measures and requests pending in this Legislature will permit ETS and the departments to significantly improve the cyber security of State government. ETS respectfully requests that that the Legislature consider these proposals that collectively are critical to building the State's cyber security program, which protects all three branches of government that today share a common access point to the Internet where most cyber threats originate.

> ***S.B. 2807, S.D. 2, Relating to Enterprise Technology Services***
> New language in Section 27-43, as proposed by S.B. 2807, S.D. 2, would serve to improve information technology governance and security, as requested by the Legislature in Act 119, SLH 2015.
>
> ***H.B. 2755, H.D. 2, Relating to Incident Response***
> ETS supports the passage of H.B. 2755, H.D. 2, introduced and advanced by state House of Representatives, which would add new language in H.R.S. Section 27-43.5 requiring the CIO to develop and maintain an incident response plan to cyber attacks for each Executive Branch department and sets out the scope of an incident response plan.

Cybersecurity Briefing — In consideration of the sensitive nature of the State's cyber security measures, ETS on February 11 provided a secure briefing for members of the House Committee on Veterans, Military, and International Affairs, and Culture and the Arts, which was considering this bill. Committee members were briefed on the architecture of the State network, relation to other networks, scope of current threats, what we monitor, and ongoing cybersecurity strategy and efforts.

H.B. 1700, H.D. 1, Relating to the State Budget

Additional skilled security positions and funds are being requested to carry out provisions of the above bills and to perform 24/7/365 cyber security functions that are now conducted only during regular business hours due to limited staff. Priority items within the budget request relevant to cybersecurity include the following:

- **Five (5) cybersecurity positions**
  Following the purchase of the State security contract in fiscal year 2015, ETS was advised that a continued use of equipment acquisition funds for the purpose of maintenance and operations was not an appropriate use. Consequently, under the current CIO's leadership, the State has been able to shift a majority of work being done by contractors to State personnel by providing additional training to the employees. Furthermore, the State has moved into new partnerships with the U.S. DHS and the FBI to rely on their expertise and resources to further secure the environment.

  This shift has reduced the number of people working on cyber security down from four consultants and four staff, to one consultant and three staff. While this has saved the State more than $1 million dollars per year, these positions are needed to rebuild support. The focus of the existing staff is to focus on perimeter security and the next phase to build the endpoint (desktop) security platforms. The additional staff will be needed to help departments secure their endpoints and to proactively search for vulnerabilities in our network (not being done today).

- **One (1) Chief Security Officer**
  The creation of this lead position, along with security engineer positions requested, will fill resources and knowledge gaps critically needed to confront growing cyber security dangers. The Chief Security Officer will create standards and best practices for the state, which will include the new responsibilities in H.B. 2755 H.D. 2 to create cyber incident response plans for each department.

  Without this position to develop and lead a comprehensive statewide cyber security program, the state faces increasing risks of successful cyber attacks and the millions of dollars in damages and expenses to comply with security breach notification from losses of confidential personally identifiable information (PII). Each day, the State network witnesses millions of potential Internet security threats, which continues to grow in quantity and sophistication. Without a cyber security program in place, government agencies will eventually fall victim to this new form of terrorism.

- **Nine (9) Information Management and Technology Services positions**
  These positions will eventually reduce or eliminate the need for the many consultants currently supporting the Hawai‘i Government Private Cloud (GPC). In place of those consultants, these System Engineers will perform essential IT security and governance services in support of statewide enterprise programs.

  Without these Systems Engineer positions, the reliance on costly external consultants and vendors will continue.

- **$150,000 in general funds for anti-virus software licenses for transformation initiatives**
  This funding request includes renewing security software licenses in departments, and acquiring new licenses for desktops with outdated or inadequate security software.

  Without funding for anti-virus and anti-malware software licenses for all departments, the State network, applications and thousands of individual computing devices face increasing risks of cyber attacks and loss of data.