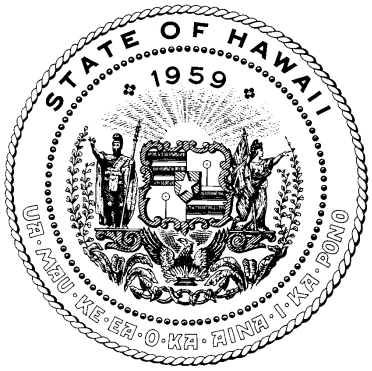

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

QUARTERLY REPORT ON

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

OCTOBER 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
October 2016

The Office of Enterprise Technology Services (ETS) submits the following quarterly report, pursuant to Section 42(5) of Act 119, Session Laws of Hawaiʻi (SLH) 2015.

In consideration of the sensitive nature of cybersecurity, ETS is available to the Legislature upon request to provide a more detailed briefing, in a secure environment, regarding the contents of this report.

Background

In referencing Hawaiʻi Revised Statutes Sections 26-6 and 27-43.5, Act 119 of 2015 reaffirms the authority of ETS (formerly the Office of Information Management and Technology), as led by the Chief Information Officer (CIO), over centralized cybersecurity of Executive Branch systems. Section 27-43.5 refers to periodic security audits of all Executive Branch departments and agencies regarding the protection of government information and data communication infrastructure.

Since 2015, additional legislation was enacted to further strengthen the CIO's authority with regard to IT security governance. Specifically, new language added to Senate Bill 2807 SD2, Relating to Enterprise Technology Services (now Act 58, SLH 2016), authorizes the CIO, effective July 2, 2016, to coordinate each Executive Branch department and agency's IT budget request to ensure compliance … with ETS' IT governance processes and enterprise architecture policies and standards, including policies and standards for systems, services, hardware, software, and *security* management.

- ETS is collaborating with the Department of Budget and Finance (B&F) to exercise enhanced IT governance authority as part of the upcoming budget preparation process prior to the 2017 legislative session. ETS and B&F on Sept. 16, 2016, issued a joint memorandum to department heads providing guidelines for submitting IT and information resource management roadmaps and new biennium budget request documents for review and approval by both ETS and B&F.

Additionally, the Legislature's approval of three new cybersecurity positions will help further build 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. These new positions will also allow ETS to pursue cost-effective solutions for Hawaiʻi's cybersecurity needs by providing additional training to State employees. Training employees enables the State to shift a majority of security work previously done by contractors to skilled State personnel.

- ETS is in active recruitment for the following new cybersecurity positions approved in the 2016 legislative session:

- Chief Information Security Officer (CISO) — for establishing security standards and to ensure that the State stays current with best practices in security.
- Two cybersecurity support positions — for operations (The focus of existing staff has been on perimeter security and the next phase to build the end-point security platforms. These additional staff will help departments secure their endpoints and to proactively search for vulnerabilities in the network).

Approach to Cybersecurity

As reported in previous quarterly reports to the Legislature, 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. The status of a variety of these measures is provided below.

On-Going Vulnerability Assessments. ETS regularly conducts internal and external vulnerability scans to identify vulnerable devices within the State's Next Generation Network.

Federal Cyber Hygiene Scans. Cyber hygiene scans of departments and agencies, conducted by partnership the U.S. Department of Homeland Security (U.S. DHS) and the FBI as part of the Federal Cyber Hygiene (CyHy) program, provide snapshots of cybersecurity risk.

The State has been a CyHy program participant since 2014, receiving network vulnerability scanning of external-facing public IP addresses to help the State understand how it appears to attackers on the Internet. State departments and agencies review and take appropriate corrective action.

- ETS continues to work with its Federal partners to take advantage of CyHy program resources.

- ETS this year increased the frequency of the distribution of CyHy program scan results from monthly to nearly weekly, providing significantly more up-to-date status of department vulnerabilities to State IT personnel.

Internal Assessments. ETS this year purchased MS-ISAC vulnerability assessment for testing internal Executive Branch infrastructure for various vulnerabilities. To extend security support into the departments:

- ETS made vulnerability management tools available to departments to perform their own vulnerability assessments of their assets. Rollout is ongoing.

Security Device Monitoring: Netflow Monitoring & Analysis

Federally funded Netflow Monitoring and Analysis from the Center for Internet Security (CIS) / Multi-State Information Sharing & Analysis Center (MS-ISAC) is an automated process of collecting, correlating and analyzing computer network security information across State

governments. The seven key Netflow fields are: source IP address, destination IP address, source port number, destination port number, protocol type, flags, and the router input interface. Services available to the State include security event analysis and notifications 24x7, technical assistance, remediation consulting. Security events spanning thousands of desktops and servers are analyzed and correlated for alerting and/or action.

Local Enterprise Security Information and Event Management

The Security Information and Event Management (SIEM) system collects and analyzes thousands of security events and logs from internal monitoring points.

Alerts and notices are transmitted to Data Processing Coordinators and IT Governance Technical Committee members for remedial action and to use in security awareness programs.

- To facilitate remedial action, as appropriate, ETS this year launched a new ticket system by which identified vulnerabilities may be expeditiously resolved by departments. After review and implementation of mitigation measures, departments/agencies may request supplemental scans conducted to validate issues have been remediated.

- To fortify the State's secure Wi-Fi infrastructure, ETS added new software and hardware, and account management procedures.

Data Loss Prevention

Data loss prevention (DLP) protects against data leakage key capability to support State privacy protection efforts, e.g., social security numbers and other personally identifiable information (PII).

- Enhanced DLP has been a benefit of the transition of the majority of Executive Branch departments to the Microsoft Office 365 platform over the past year. As of the date of this report, ETS has worked with departments to successfully deploy more than 12,400 Office 365 user licenses — along with the many tools and enhanced resources now available to State personnel.

Additional Microsoft tools and resources are being implemented to further improve security:

- Piloted the Microsoft Enterprise Mobility Suite (near completion) so departments can manage their mobile devices. This will go into production in 2016.
- Removed end-of-life mail security devices and migrated to Office 365.
- Purchased additional persistent adversary detection service, which will be implemented in the later part of 2016. A team of Microsoft security specialists will analyze the Microsoft infrastructure for the Executive Branch for security vulnerabilities and intrusions.
- Developed procedures, and a playbook, for the deployment of security and management of software tools, not only for use by ETS, but also for other departments that need such resources.
- Developed and communicated a process by which all State Office 365 email users can encrypt their email, sent to external users, simply by typing *secure* in the subject line.

Expansion of End-Point Security

Providing updated anti-virus and anti-malware software for thousands of individual computing devices in all departments reduced risks of cyber attacks and loss of data.

This year, ETS:

- Funded from its operating budget the renewal of security software licenses for departments statewide using desktop devices that had outdated or inadequate security software.

- Added anti-ransomware software through its Malwarebytes purchase.

- Deployed end-point management tools into the departments.

The following illustrates the wide range of security services and tools that ETS integrated to further secure the State's computing environment: