OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

QUARTERLY REPORT ON

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

JULY 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
July 2016

The Office of Enterprise Technology Services (ETS) submits the following quarterly report on 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.

Enhancement of IT Security Governance

Since the last quarterly report was submitted on April 1, 2016, legislation passed to further strengthen the State of Hawaiʻi Chief Information Officer's (CIO) authority with regard to IT security governance.

Currently, cybersecurity authorities and responsibilities within State of Hawaiʻi government are outlined in statute as follows:

HRS §27-43	Establishes the State 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

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 information technology (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 will collaborate with the Department of Budget and Finance to exercise this new authority as part of the upcoming budget preparation process prior to the 2017 legislative session.

Approach to Cybersecurity

As previously reported, 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 following cybersecurity efforts continue:

- Federally funded "Managed Security Services" from the Center for Internet Security (CIS) / Multi-State Information Sharing & Analysis Center (MS-ISAC) provide the capability to monitor and respond to threats and attacks on the 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 analyzes 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 Coordinators and IT Governance Technical Committee members, for remedial action and to use in security awareness programs.

ETS has purchased the MS-ISAC vulnerability assessment for testing Executive Branch infrastructure for various vulnerabilities.

Office 365 Continues to Augment End-Point Security

The transition of the majority of Executive Branch departments to the Microsoft Office 365 platform has fortified security and increased disaster recovery capability. As of the date of this report, ETS has worked with departments to successfully deploy more than 12,000 Office 365 user licenses — along with the many tools and enhanced resources now available to state personnel.

The following are additional Microsoft tools and resources that have or are being implemented to further improve security:

- Expanded data-loss prevention (DLP) infrastructure with Microsoft Office 365 DLP.
- Piloted the Microsoft Enterprise Mobility Suite (near completion) so departments can manage their mobile devices. This will go into production this calendar year.
- 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 email users can encrypt their email, sent to external users, by typing in *Secure* in the subject line.

Increased Frequency of Cyber Hygiene Scans

ETS continues to work with the U.S. Department of Homeland Security (DHS) and FBI to take advantage of other Federal resources and expertise, including DHS' Cyber Hygiene (CyHy) program. Since 2014, the State has been a CyHy participant, 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 are provided scan results, which are provided individually and securely to departmental IT leads or other designated personnel to review and act on.

ETS is increasing frequency of reporting to departments on the vulnerabilities of Internet facing assets. Since the last quarterly report to the Legislature, ETS has increased the frequency of scans result distribution from monthly to nearly weekly, providing significantly more up-to-date status of department vulnerabilities to IT personnel.

Launch of New Ticket System

To facilitate remedial action, as appropriate, ETS last quarter 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 (outside the regular schedule of the CyHy program) to validate issues have been remediated.

Expanded End-Point Security

ETS funded from its operating budget the renewal of security software licenses for departments statewide and acquisition of new licenses for desktops with outdated or inadequate security software. Without anti-virus and anti-malware software licenses for all departments, the State Network along with applications and thousands of individual computing devices faced increased risks of cyber attacks and loss of data.

ETS likewise acquired the following to further secure state devices:

- Purchased and implemented additional vulnerability management tool so departments can perform their own vulnerability assessments of their assets. Rollout is ongoing.
- Purchased and is in the process of deploying end-point management tools for imaging, and software deployment, for ETS. These can also be used for other departments.
- Purchased other software licenses and hardware to implement, and fortify, the State WiFi infrastructure.

New Cybersecurity Positions

In submitting ETS' supplemental budget request for the 2016 legislative session, the agency placed a high priority on cybersecurity. The addition of skilled security specialists was identified as a pressing security need.

The Legislature's approval of three new cybersecurity positions will help to improve the effectiveness of the above efforts and in the building of 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 Hawai‘i'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.

As the new fiscal year begins, ETS will immediately begin recruitment for the following new cybersecurity positions approved during the 2016 session:

- **Chief Information Security Officer** (CISO) — to establish security standards and 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 our network).