OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

QUARTERLY REPORT ON

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

APRIL 2017

SUBMITTED TO

THE TWENTY-NINTH STATE LEGISLATURE

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES
STATE OF HAWAI‘I

Quarterly Report on Periodic Information Security and Penetration Audits
of the Executive Branch Information Technology Systems
April 2017

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

BACKGROUND

In referencing Hawai‘i Revised Statutes (HRS) sections 26-6 and 27-43.5, Act 119 of 2015 reaffirms the authority of ETS, as led by the Chief Information Officer (CIO), over centralized cybersecurity of executive branch systems. Statutorily mandated information technology (IT) governance, management and security duties include those listed below.

Summary	Statutory Reference
Provide centralized computer information management and processing services.	HRS section 26-6
Coordinate each executive branch department and agency’s information technology budget request, forecast, and procurement purchase to ensure compliance with the department or agency’s strategic plan and road map and with ETS’ IT governance processes and enterprise architecture policies and standards, including policies and standards for systems, services, hardware, software, and security management.	HRS section 27-43
Provide for periodic security audits of all executive branch departments and agencies regarding the protection of government information and data communication infrastructure.	HRS section 27-43.5
Set policies, procedures and standards for each executive branch department’s reasonable efforts to make appropriate and existing electronic data sets maintained by the department electronically available to the public through the State’s open data portal at data.hawaii.gov or successor website.	HRS section 27-44
Provide services through centralized web portal and Internet presence (hawaii.gov) that allow citizens to conduct business electronically with the government, in accordance with statute (i.e., Access Hawai‘i Committee).	HRS chapter 27G
Provide guidance to protect personal information that is collected and maintained by State and county government agencies (i.e., Information Privacy and Security Committee).	HRS chapter 487N

STATE EMPLOYEE-LED CYBERSECURITY PROGRAM

The 2016 Legislature's approval of three new cybersecurity positions, including a Chief Information Security Officer (CISO), is helping to further build the State's cybersecurity 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. The State IT security team can then assist departments in further securing their endpoints and proactively searching for vulnerabilities on the State Next Generation Network (NGN).

As previously reported, ETS in December 2016 announced the hiring of O‘ahu resident Vincent Hoang as the State CISO. Hoang is responsible for establishing cybersecurity standards for the executive branch and ensuring that system operations stay current with best practices (See the news release at ets.hawaii.gov).

- With Mr. Hoang in place, ETS has also filled one of the new support positions since the last quarterly report and anticipates filling the second support position by the end of the current fiscal year — bringing the ETS IT security team to a total of seven personnel.

IT SECURITY GOVERNANCE

As stated above, HRS section 27-43, as amended by Act 58, SLH 2016, explicitly authorizes the CIO 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."

Following the effective date of Act 58, ETS in fourth quarter 2016 collaborated with the Department of Budget and Finance (B&F) to exercise this enhanced IT governance authority as part of the preparation process for the Executive Budget Request for the Fiscal Biennium (FB) 2017-2019.

- ETS has since provided input and feedback to B&F on departmental IT requests for the biennium budget submittal, and reviewed and evaluated those IT requests against established criteria. ETS also established a contract management process, where draft requests for proposals and draft vendor contracts for enterprise IT projects and initiatives are reviewed for best practices.

Moving forward, ETS will continue to refine governance processes for IT projects and, in conjunction with B&F, further institutionalize the process into the annual budget request process, enabling the integration of information into the State's overall IT strategic plans and roadmaps.

APPROACH TO CYBERSECURITY

As stated 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.

CIS/MS-ISAC Services

To supplement its internal resources, ETS continued to take advantage of a variety of monitoring and assessment services from The Center for Internet Security (CIS), Multi-State Information Sharing and Analysis Center (MS-ISAC), which the U.S. Department of Homeland Security (DHS) has designated as the coordinating entity for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments.

The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response for the SLTT community.

In addition, MS-ISAC staff sit in DHS' National Cybersecurity and Communications Integration Center (NCCIC), a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal government, intelligence community, and law enforcement.

Federal Cyber Hygiene Scans

Cyber hygiene scans of departments and agencies, conducted by the U.S. Department of Homeland Security (U.S. DHS) and the FBI as part of the Federal Cyber Hygiene (CyHy) program, continue to provide useful snapshots of cybersecurity risk. The State of Hawai'i 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.

In 2016, ETS 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. ETS continues to work with its Federal partners to take advantage of CyHy program resources.

Internal and External Vulnerability Assessments

With the increased capacity of the IT security team, ETS continues to improve the effectiveness of regular internal and external vulnerability scans to identify vulnerable devices within the State NGN, which is the State government network that serves all three branches.

Internal Assessments

In 2016, ETS 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 remains ongoing.

EDUCATION

STATE OF HAWAII 1959
ETS
OFFICE OF ENTERPRISE TECHNOLOGY SERVICES
Proclamation
In Recognition of
Cyber Security Awareness Mo

Last year, Gov. David Ige proclaimed October 2016 Cyber Security Awareness Month in Hawai‘i, highlighting the State’s vital role in identifying, protecting its citizens from, and responding to cyber threats that may have significant impact to individual and collective security and privacy. Hawai‘i’s observance coincides with National Cyber Security Awareness Month, recognized by the U.S. DHS, MS-ISAC, the National Association of State Chief Information Officers, and the National Cyber Security Alliance.

Following up on this educational opportunity, ETS disseminated cyber tips via State email and websites, social media, and ETS’ electronic newsletter, *howz.IT*. Messages emphasized that cybersecurity remains a shared responsibility in which every citizen has a critical role to play. Materials highlighted the following:

- Why Strong, Unique Passwords Matter
- Two-Factor Authentication
- Phishing Emails and You
- Cyber Tips for Students

Additionally, the ETS is working with departmental IT staff on a variety of exercises to improve cybersecurity skillsets and capability of State personnel/teams.

BENEFITS OF MICROSOFT OFFICE 365

Built-In Tools and Features

Greater IT security protection is a benefit of the transition of the majority of executive branch departments to the Microsoft Office 365 platform over the past two years. ETS has worked with departments to successfully deploy more than 12,240 Office 365 user licenses currently in use — along with the many tools and enhanced resources now available to State personnel.

Office 365 IT security benefits include:

- Data loss prevention (DLP) protects against data leakage, e.g., Social Security numbers and other personally identifiable information (PII).
- Security and management of software tools, providing better activity monitoring, patching, and access control.
- Enhanced encryption, such as ability of all State Office 365 email users to encrypt their email sent to external users simply by typing *secure* in the subject line.
- Microsoft System Center Configuration Manager and endpoint protection so departments can better manage their endpoints.

ETS is also piloting Microsoft Enterprise Mobility Suite so departments can manage their mobile devices.

Microsoft Persistent Adversary Detection Service

ETS last year conducted the first-ever statewide security assessment and scan of all Windows-based devices. Persistent Adversary Detection Service (PADS) is a service offering for proactive Microsoft clients who are looking to reduce the risk posed by targeted attacks from determined human adversaries and sophisticated criminal organizations. This includes proactive, discreet incident response prior to an actual emergency, examining assets and systems for signs of advanced implants not typically found by commodity anti-virus or intrusion detection system technologies.

PADS was implemented in fourth quarter 2016 with most departments participating. More than 12,000 endpoints (e.g., servers, desktops and laptops) were assessed/scanned.

OTHER CONTINUING PROGRAMS AND INITIATIVES

Security Device Monitoring: NetFlow Monitoring & Analysis

Federally funded NetFlow Monitoring and Analysis from CIS/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, and 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 in 2016 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.

Expansion of Endpoint Security

ETS is providing updated anti-virus and anti-malware software for thousands of individual computing devices in all departments to reduce risks of cyber attacks and loss of data. The office funded from its operating budget the renewal of security software licenses for departments statewide using desktop devices that had outdated or inadequate security software. This included added anti-ransomware software through this purchase. Efforts continue to deploy endpoint management tools into the departments.

ETS ACTIVITIES IN THE MONTHS AHEAD

Over the course of the next biennium, among ETS' top activities will be remediation of Internet-facing vulnerabilities, patch management on endpoint, and efforts to work with departmental IT staff on exercises to improve cybersecurity skillsets and capability of State personnel/teams.

Additionally, as resources allow, ETS will enhance internal vulnerability scanning and building upon proactive investigation capabilities for identified and unidentified threats.

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.