OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

QUARTERLY REPORT ON

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

JANUARY 2017

SUBMITTED TO

THE TWENTY-NINTH 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
January 2017

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, 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.

IT SECURITY GOVERNANCE

During the 2016 legislative session, 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.

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

  This follows a joint ETS/B&F memorandum, sent on September 16 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. Specifically, departments and agencies were required to develop and maintain their multi-year IT strategic and tactical plans and roadmaps along with their budget request submittals for consideration as part of the State's overall IT strategic plans, roadmaps, and directions.

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. In addition, "Exhibit A" provides an illustration of the wide range of security services and tools that ETS employs to secure the State's computing environment.

CIS/MS-ISAC Services

To supplement its internal resources, ETS receives 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, provide 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. ETS in 2016 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.

Ongoing Vulnerability Assessments

ETS regularly conducts internal and external vulnerability scans to identify vulnerable devices within the State's Next Generation Network (NGN), the State government network that serves all three branches.

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 remains ongoing.

STATE-EMPLOYEE LED CYBERSECURITY PROGRAM

The 2016 Legislature's approval of three new cybersecurity positions, including a Chief Information Security Officer (CISO), will help 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.

- In December 2016, ETS announced the hiring of O'ahu resident Vincent Hoang as the State CISO. In place since December 1, 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). Mr. Hoang is actively participating in the hiring of the two cybersecurity support positions, who will assist departments in further securing their endpoints and proactively searching for vulnerabilities in the State NGN. The focus of existing staff thus far has been on perimeter security, and the next phase is building endpoint security platforms.

EVENTS OF NOTE

Microsoft Persistent Adversary Detection Service

As stated in the last quarterly report, ETS purchased additional persistent adversary detection service (PADS) with plans to implement in fourth quarter 2016. PADS is a service offering for proactive clients who are looking to reduce the risk posed by targeted attacks from determined human adversaries and sophisticated criminal organizations.

- In fourth quarter 2016, ETS conducted the first statewide security assessment and scan of all Windows-based devices, which was offered to all executive branch departments, including the Department of Education and the Library System. ETS received participation from most departments. The service provided 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.

Hawai'i State Elections

ETS participating in a multi-agency effort to secure the State's elections and ensure that the voter registration database and process remained secure.

- In support of the Office of Elections, ETS successfully coordinated with the Department of Homeland Security, FBI, and Hawai'i State and county agencies.

Cyber Security Awareness Month

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.

- Throughout the month, ETS provided weekly cyber tips to State employees as well as the general public, disseminated 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

Hawai‘i's observance coincides with National Cyber Security Awareness Month, recognized by President Barack Obama, the U.S. Department of Homeland Security, the Multi-State Information Sharing and Analysis Center, the National Association of State Chief Information Officers, and the National Cyber Security Alliance. In addition, the annual national cybersecurity public awareness campaign "Stop.Think.Connect." is implemented through a coalition of private companies, nonprofit and government organizations, as well as academic institutions working together to increase the understanding of cyber threats and empower the American public to be safer and more secure online.

OTHER 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, 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.

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. ETS has worked with departments to successfully deploy approximately 12,390 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. ETS in conjunction with departments: removed end-of-life mail security devices and migrated to Office 365; 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; developed procedures and processes to deploy Microsoft System Center Configuration Manager and endpoint protection so that interested Departments can better manage their endpoints at no additional costs to them.

- In fourth quarter 2016, ETS piloted the Microsoft Enterprise Mobility Suite (near completion) so departments can manage their mobile devices.

Expansion of Endpoint Security

ETS is 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; and
- deployed endpoint management tools into the departments.

EXHIBIT A:
Security Services and Tools ETS Employs to Secure the State's Computing Environment