DAVID Y. IGE
GOVERNOR

TODD NACAPUY
CHIEF INFORMATION
OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES
P.O. BOX 119, HONOLULU, HAWAI'I 96810-0119
ETS.HAWAII.GOV

OFFICE OF INFORMATION MANAGEMENT
AND TECHNOLOGY

INFORMATION AND COMMUNICATION
SERVICES DIVISION

December 31, 2015

The Honorable Ronald D. Kouchi,
President, and
Members of the Senate
Twenty-Eighth State Legislature
State Capitol, Room 409
Honolulu, Hawai'i 96813

The Honorable Joseph M. Souki,
Speaker, and Members of the House of
Representatives
Twenty-Eighth State Legislature
State Capitol, Room 431
Honolulu, Hawai'i 96813

Dear President Kouchi, Speaker Souki and Members of the Legislature:

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

In accordance with HRS §93-16, this notice may be viewed electronically at http://ets.hawaii.gov.

Sincerely,

Todd Nacapuy

TODD NACAPUY
Chief Information Officer
State of Hawai'i

(1) Attachment

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
January 1, 2016

The Office of Enterprise Technology Services submits this third 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 Hawai'i (SLH) 2015.

Background

Due to the sensitive nature of the State's cyber security measures, compounded by the requirement to post reports electronically in accordance with Hawai'i Revised Statutes §93-16, ETS sought input from members of the Senate and House of Representatives to clarify means of reporting in order to safeguard data, personally identifiable information (PII) and other sensitive information entrusted to departments and agencies.

Upon full consideration of feedback, including input from the Chairs of the Senate Committee on Economic Development, Environment and Technology (EET) and House Committee on Economic Development and Business (EDB), ETS has satisfied its concerns and provides the following "high-level" report. Should additional detail be required, the CIO and his cyber security team are available upon request to provide a classified briefing.

Periodic Information Security and Penetration Audits

Since 2014, the State has partnered with the U.S. Department of Homeland Security Cyber Hygiene Program, which provides network vulnerability scanning of external-facing public IP addresses to help the state understand how it appears to attackers on the Internet. As part of the program, State departments and agencies are provided scan results, which are provided individually and securely to departmental CIOs or other designated personnel to review and act on. The information includes a rating of vulnerabilities on a scale of 1 to 4, where 4 indicates a critical vulnerability that should be addressed immediately.

In addition, the State's Security Operations Center (SOC), established in 2014, possesses the ability to conduct additional vulnerability scans against the State's assets to further supplement the CyHy program and provide direct operational support to departments assess the vulnerability status of their public-facing assets. 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. The SOC staff has been concentrating on operational and project work activities as the SOC team transition to State personnel.

Recommendations and Remedial Action

The SOC regularly notified departments/agencies of vulnerabilities found in applications ranging from word processing software to web browsers. Since July 2015, the SOC has issued 47 notices of various vulnerabilities and recommendations for remedial action.

Cyber Security Public Awareness

Maintaining the security of cyberspace is a shared responsibility in which everyone has a critical role to play. The following public awareness activities were conducted to educate State personnel as well as the public on best practices.

Cyber Security Awareness Month

Recognizing the State of Hawai'i's vital role in identifying, protecting and responding to cyber threats, Gov. David Y. Ige proclaimed October "Cyber Security Awareness Month" in Hawai'i. The observance coincided with National Cyber Security Awareness Month, recognized by President Barack Obama and various public and private sector agencies to encourage all citizens to learn about cyber security and put that knowledge into practice in their homes, schools, workplaces and businesses.

To raise public awareness nationwide, the annual Stop.Think.Connect. campaign empowers the American public to take security precautions, understand the consequences of online actions and behaviors, and enjoy the benefits of the Internet. For additional cyber security resources throughout the month as well as year-round, State personnel as well as the general public were encouraged to visit www.stopthinkconnect.org and the State Cyber Security Team webpage at http://ags.hawaii.gov/icsd/cyber-security.

Cyber Security Tips Newsletter

The SOC also issues a monthly Cyber Security Tips Newsletter to Data Processing (DP) Coordinators and IT Governance Technical Committee members, who are encouraged to take advantage of the information and use them in their own security awareness programs.

Since July 2015, newsletters have focus on the following topics:

- December 2015 – Getting Your Device and Checking It Twice
- November 2015 – Safe Online Holiday Shopping
- October 2015 – Malware Wears Costumes, Too
- September 2015 – New Credit Card Chip Technology
- August 2015 – The Harm in Password Reuse
- July 2015 – Sun, Sand, and Cyber Security

The newsletters are available online at:
http://ags.hawaii.gov/blog/category/cyber-security-newsletters/

Center for Internet Security (CIS) / Multi-State Information Sharing & Analysis Center (MS-ISAC)

The State is also increasing utilization of resources offered by CIS / MS-ISAC, which is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments – a collaborative effort among the SLTT and the U.S. DHS. The MS-ISAC has been designated by U.S. DHS as the key resource for cyber threat prevention, protection, response and recover for the nation's state, and local governments.

MS-ISAC Security Operations Center
The MS-ISAC 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

Security Device Monitoring – Managed Services
Managed Security Services (MSS) includes monitoring IDS and IPS security devices and providing event analysis and technical assistance.

Security Device Monitoring – Netflow
Netflow Monitoring and Analysis (Albert) is an automated process of collecting, correlating and analyzing computer network security information across State governments. The service also provides technical assistance and remediation consulting.

Incident Response
The Center for Internet Security (CIS) and its Cyber Emergency Response Team (CERT) assists partners in analyzing security information to assess the scope, magnitude, and source of intrusion when a cyber event is reported:

Network & Computer Forensic Analysis

- Log & Malware Analysis
- Access to the Malicious Code Analysis Platform (MCAP)
- Remediation Consulting
- Leverage Additional Resources through the National Cybersecurity and Communications Integration Center

Threat Notification
CIS Analysts and trusted third parties conduct research that provides intelligence in regard to targeted threats and release of information from compromised government or government affiliated systems and website defacements.

- Notices are sent to the impacted partners based on predetermined escalation procedures
- Recommended remediation steps are provided
- CIS Analysts are available for technical assistance

More CIS-CAT Services Coming in 2016
The State of Hawai'i will implement additional CIS services, such as security benchmark analyses, network configuration assessments, vulnerability assessments of public facing services, penetration testing, web allocation assessments, and cyber security awareness training.