DAVID Y. IGE
GOVERNOR

TODD NACAPUY
CHIEF INFORMATION
OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119
Ph: (808) 586-6000 | Fax: (808) 586-1922
ETS.HAWAII.GOV

INFORMATION AND COMMUNICATION
SERVICES DIVISION

OFFICE OF INFORMATION MANAGEMENT
AND TECHNOLOGY

December 17, 2015
DRAFT

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:

On behalf of Information Privacy and Security Council, which is assigned to the Department of Accounting and General Services and chaired by the State Chief Information Officer, the Office of Enterprise Technology Services respectfully submits this report on procedures of notification following the breach of personal information, pursuant to S.C.R. 88 of the 28th Legislature of the State of Hawaii, Regular Session of 2015.

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

Sincerely,

TODD NACAPUY
Chief Information Officer
State of Hawai‘i

(1) Attachment

Information Privacy and Security Council

Report on Procedures of Notification following the Breach of Personal Information

Background

Individual personal information is increasingly stored online or in electronic format. In addition to establishing the Information Privacy and Security Council (IPSC), HRS §487N sets out procedures for State and county government agencies to report to the Legislature certain information after discovery of a security breach. The information required to be reported includes information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring

Despite statutory requirements for providing notice of breaches as well as ongoing efforts by the IPSC to make recommendations to protect personal information used by government agencies, S.C.R. 88 noted that further improvements to the notification process are necessary. The resolution requested that IPSC, in cooperation with the State CIO Council, assess the means by which State and county agencies generally notify individuals following a breach of personal information, and research and provide a report to the Legislature with its findings.

The IPSC's report follows:

1. Notification procedures currently followed when contacting and notifying an individual about the breach of personal information, particularly when the personal information is stored or accessible online

The IPSC consulted with the Office of Consumer Protection (OCP) of the Department of Commerce and Consumer Affairs (DCCA) to discuss OCP practices regarding the receipt of data breach reports.

State law requires government agencies to submit a written report to the legislature within 20 days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. In the event that a law enforcement agency informs the government agency that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

State law requires businesses to report data breaches of 1,000 or greater to OCP, based on the number of individuals required to be notified. This is a relatively high threshold amongst states. Hawai‘i shares this threshold with Missouri and South Carolina, while the threshold for California, Florida, and Iowa is 500. Approximately 12 states have no threshold for reporting (meaning all breaches are reported).

According to OCP, the number of reported incidences in Hawai‘i involving more than 1,000 individuals totaled six in 2014 and eight in 2015 (as of October 2015). Although not required, OCP provides this information to the Federal Trace Commission (FTC).

To address the concerns of S.C.R. 88, the IPSC considered legislative amendments requiring OCP to post the information on a central website to make information about breaches available to potentially impacted individuals who may not be easily reached due to change of address or other reasons. OCP confirmed that individuals typically check with OCP or the entity involved. Counties, if contacted, tend to refer inquires to OCP.

However, as the information reported to OCP is publically available and the office already has the power to post said information, IPSC recommends against placing this requirement in statute, as it may have unintended consequences. Many entities, as a general practice, proactively inform every state based on the lowest threshold among them nationwide. If put in law, this may discourage businesses from reporting incidents that are under the threshold. Requiring it in statute may inadvertently restrict the state from listing those under 1,000.

The proposed amendment requiring credit monitoring/protection was also discussed. While a breach involving a public or private entity does not require credit monitoring, OCP affirmed that it is a common practice by businesses as part of good customer relations. The cost of credit protection ranges from an estimated $7 to $25 per person annually. California requires private businesses to offer credit monitoring/protection, but this requirement does not apply to states. Their thought was that requiring it of state agencies by law could present risk for unbudgeted liability to taxpayers. A sizable breach could result in millions of dollars to taxpayers. OCP was not aware of any complaints received regarding lack of credit monitoring/breach protection offered by our state agencies.

It is also worth noting that draft Privacy Risk Management framework from the National Institute of Standards and Technology (NIST), which applies to federally funded projects or federal data partners that are subject to audit, is in a period of review.

2. Software or other electronic programs generally used that foster improvement of personal information protection; and

The IPSC has identified the following resources for information security, and has made this list available on its publicly accessible website (http://ipsc.hawaii.gov).

No endorsement is implied or intended by the State of Hawai‘i by the listing or omission of vendors and/or commercial products on this page.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

- The MS-ISAC Nationwide Cyber Security Review is a voluntary self-assessment survey designed to evaluate cyber security management. It is available to all states and agencies, local government and departments, and tribal and territorial governments: https://msisac.cisecurity.org/resources/

Free/Open Source Tools

- Vulnerability Scanning

- Secunia PSI: http://secunia.com/vulnerability_scanning/personal/
- OpenVAS: http://www.openvas.org/
- Microsoft Baseline Security Analyzer: http://www.microsoft.com/en-us/download/details.aspx?id=7558
- Qualys FreeScan (online vulnerability scanner – need to sign up): https://www.qualys.com/forms/freescan/

Website Safety Rating
The following are web-based tools to help identify if a site is safe or unsafe.

- McAfee Site Advisor adds visible safety ratings to searches and sites visited
- Norton (Symantec) Safe Web allows you to enter a web address (URL) and will return a rating based on safety and security issues

Browser Plug-in Check
Web-based, simple to use, free tool to check your browser for outdated plug-ins.

- The Qualys Browser Check will identify outdated plug-ins that may be vulnerable to attacks

Useful Firefox Plug-ins

- Better Privacy deletes super-cookies
- NoScript prohibits potentially harmful scripts from being executed within a web page

3. Recommendations of amended or new methods to more securely and promptly provide notification.

The IPSC provides the following recommendations:

- The OCP should post breaches of which it is notified on a central breach information portal be maintained by the office. The counties should be encouraged to post a link to this site.

- Under an enterprise license agreement administered by the DAGS Risk Management or the Office of Enterprise Technology Services, the State should obtain "cyber insurance" for State of Hawaii agencies.

- Government agencies should fully adopt the federal guidelines provided under the National Institute of Standards and Technology (NIST) Privacy Risk Management framework, once finalized. To better anticipate and address the impacts these technologies can have on privacy in federal information systems, NIST has drafted a document that lays out a framework for privacy risk management and is asking for public comment on the draft framework. In developing the draft Privacy Risk Management Framework, NIST sought the perspectives and experiences of privacy experts across a variety of sectors in an open and transparent process that included workshops, public comment periods and various other outreach activities. Collected input will be used to refine the framework.

- Amend HRS §487N-2 to statutorily require that threshold for reporting breaches to OCP be lowered from 1,000 to 500 to align with other states:

  (f) In the event a business provides notice to more than [~~one thousand~~] five hundred persons at one time pursuant to this section, the business shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. section 1681a(p), of the timing, distribution, and content of the notice.

- Amend HRS § 478N-5 so that the CIO versus the Comptroller may exempt employees to support information privacy and security, an ability more appropriately assigned to the CIO now that the position has been established:

  (e) The [~~comptroller~~] chief information officer may establish support positions [~~for the information and communication services division~~] exempted from chapters 76 and 89, including but not limited to, legal support, information technology security, human resources and personnel, records management, and administrative support.