



Information Privacy and Security Council

Meeting Minutes

December 21, 2016

Kalanimoku Bldg.
Basement VCC
1151 Punchbowl St.
Honolulu, HI 96813

Wailuku State Office Bldg.
Third Floor VCC
54 South High St.
Wailuku, HI 96793

Lihu'e State Office Bldg.
Basement VCC
3060 'Eiwa St.
Lihu'e, HI 96766

Hilo State Office Bldg.
Basement VCC
75 Aupuni St.
Hilo, HI 96720

MEMBERS / DESIGNEES PRESENT

Member Name	Department
Nacapuy, Todd (Chair)	Office of Enterprise Technology Services (ETS)
Keane, David	Department of Human Resources Development (DHRD)
Levins, Stephen	Department of Commerce and Consumer Affairs (DCCA)
Ito, Jodi (Designee)	University of Hawai'i
Norman, Nyree	County of Kaua'i
Sherman, Karen	County of Maui
Tachikawa, Joanne	Department of Education
Tungol, Wilfredo (Designee)	Department of Health
Ung, Jules	County of Hawai'i
Yong, Lim	Department of Human Services

MEMBERS ABSENT / NOT REPRESENTED

Member Name	Department
Taniguchi, Carol	Legislature
Thornton, Kevin	Judiciary
Wong, Mark	City and County of Honolulu

MEMBERS OF THE PUBLIC OR INVITED STAFF

Name	Department
Dayton, Kevin	Honolulu Star-Advertiser
DeMello, Keith (Designee)	ETS
Hoang, Vincent	ETS
Kunimoto, Valri	Department of the Attorney General (AG)

I. Call to Order

On behalf of Chair Nacapuy, Member Designee DeMello called the December 2016 meeting of the Information Privacy and Security Council (IPSC) to order at 1:04 p.m. Quorum was established with ten members/designees present.

With many new individuals present, Member Designee DeMello asked all in attendance to introduce themselves.

Jules Ung, Hawai'i County Director of Information Technology, introduced herself as the new member representing Hawai'i County. Kevin Norris, Information Systems Program Manager, will be her designee, with Betsy Leelay, Temp Information Systems Program Manager, serving as a second alternate.

Chair Nacapuy introduced Vincent Hoang as the State's Chief Information Security Officer (CISO), a position within ETS that the Legislature approved in 2016. Now that Mr. Hoang is in place, Chair Nacapuy announced his intent to name Mr. Hoang as his designee for future IPSC meetings.

II. Review and Approval of Previous Meeting Minutes

Member Yong moved for the IPSC to approve the November 2016 meeting minutes, and Member Keane seconded the motion. The IPSC adopted the minutes by unanimous consent.

III. Public Testimony on Agenda Items

None.

IV. Status of State and County Agency Personal Information (PI) System Annual Reports

Any government agency that maintains one or more personal information systems is required under HRS section 487N-7 to submit to the IPSC an annual report on the existence and character of each PI system added or eliminated since the agency's previous annual report. Member Designee DeMello summarized the status of agency reporting to date. A snapshot as of December 15 (when the December IPSC meeting agenda was posted), was included in the draft IPSC Summary Report, attached to the agenda. Since then, DeMello noted that additional agency reports were submitted, which will each be reflected in the final report. He also noted that, overall, there has been an improved rate of responses from agencies relative to 2015, and quite a few agencies are stating that they are no longer maintaining PI. This trend is encouraging, as it reduces overall risk and goes to the original intended purpose of the IPSC.

However, it was noted that there are currently quite a few agencies within Maui County that are logged as "Not Compliant." Member Sherman stated that she hopes to get some reports by the end of week but also acknowledged that there have been a lot of recent changes on Maui.

Member Designee DeMello stated that the IPSC is required to submit its annual summary report by December 29, which is twenty days prior to the start of the 2017 legislative session, and that any agencies that provide reports by December 28 will be reflected in the final report submitted to the Legislature on the following day.

Member Yong stated his appreciation of ETS for making the agency report template available as an online form this year. While it was acknowledged that the online form was significantly longer than the 2015 form (as the online form was aligned with federal reporting to increase consistency and further increase efficiency), a benefit of the online form for agencies is that information will be saved for the following year and need only be modified if updates are required. Another benefit of its being so thorough is education of agency privacy designees.

(Submissions were further discussed later in the meeting under the related topic of the Draft IPSC Summary Report to the Legislature under agenda item VI.)

V. Development of Legislative Amendments Addressing Found Media Sanitation

Members discussed the IPSC subcommittee's report and recommendations with regard to HRS section 52D-14, Duty and Right of Finders, HRS section 261-17.7 (the latter specifically addresses, and exempts from section 52D-14, lost and found money or property at airports). As discussed at previous meetings, current statutes do not appear to address electronic devices and the personally identifiable information they may contain.

In the October 2016 meeting, the IPSC voted to form a subcommittee consisting of Member Designee DeMello, Member Keane, and appropriate AG and ETS staff to develop a recommendation for legislative amendments. Initial recommendations were provided at the

November 2016 meeting for discussion, and Member Designee DeMello now presented updated recommendations, based on members' comments. Note: After the meeting agenda was posted on December 15, the State Department of Transportation (DOT) provided additional comments requesting that language allow for DOT to "dispose of" found items by public auction (as currently permitted) and clearly outline who is responsible for sanitation of found media.

As presented at the December meeting, the proposed amendments to HRS sections 52D-14 and 261-17.7, including input from DOT, were as follows:

[§52D-14] Duty and right of finders. (an) *Except as provided in section 261-17.7, all money or property found shall be reported or delivered by the finder to the chief of police of the county. When so delivered, it shall be held by the chief of police for forty-five days or until claimed by some person who establishes title or right of custody thereto to the satisfaction of the chief of police. If title or right of custody is established, the money or property shall be delivered to the claimant by the chief of police.*

(b) *If no claim is made or no such right is established within the forty-five days, the money or property shall be returned to the person who delivered it to the chief of police, except as provided in subsection (c); provided that if the person who delivered it to the chief of police fails to claim the money or property within thirty days after being notified by the chief of police that the person is entitled to possession, the chief of police shall dispose of the money or property in accordance with the procedures established in section 52D-10. For the purpose of this section, notice by regular mail to the person's last known address shall be sufficient.*

(c) Prior to being returned to the finder, an electronic device that allows for storage of personal information, as defined by section 487N-1, shall be sanitized in accordance with guidance provided by the information and privacy security council and national institute of standards and technology to ensure removal of personal information prior to returning the device to the finder. If removal of personal information is not possible or cannot be verified without unreasonable expense, the device shall be destroyed in a manner sufficient to eliminate the information, prior to disposal or recycling. The chief of police shall notify the finder that the device was destroyed and disposed of or recycled because personal information could not be removed.

§261-17.7 Lost and found money or property at airports. (an) *All money or property found at an airport owned or controlled by the department shall be reported or delivered by the finder to the airport lost and found, and when so delivered shall be held by the department for forty-five days or until claimed by some person who establishes title or right of custody thereto to the satisfaction of the department. In the event of the establishment of title or right of custody, the money or property shall be delivered to the claimant by the director or the director's agent. If within forty-five days no claimant establishes a right to the money or property, the money or property, except as provided in subsection (d) with regard to electronic devices, shall be returned to the person who delivered it to the airport lost and found; provided that if the person who delivered it to the airport lost and found fails to claim the money or property within thirty days after being notified by the director, the director shall deposit the money into the state treasury to the credit of the airport revenue fund or shall dispose of the property by public auction.*

(b) *At least once annually, the director shall give public notice giving details as to time and place of the auction and giving notice to all persons interested or claiming the*

property that unless claims are made by persons who can provide satisfactory proof of ownership before a specified date, the property will be sold at public auction to the highest bidder. On the day and at the place specified in the notice, all property for which no satisfactory proof of ownership is made shall be sold by auction by or under the direction of the director.

If any property which is of a perishable nature or unreasonably expensive to keep or safeguard remains unclaimed at the airport, the director may sell that property at public auction, at a time and after notice that is reasonable under the circumstances. The director shall immediately after the sale of any property pay to the airport revenue fund all moneys received by the director upon sale.

(c) For the purpose of this section, notice by regular mail to the last known address of the person who delivered the money or property to the airport lost and found shall be deemed sufficient.

(d) Prior to disposal of the property by public auction or other means, an electronic device that allows for storage of personal information, as defined by section 487N-1, shall be sanitized by the director or the director's agent in accordance with guidance provided by the information and privacy security council and national institute of standards and technology to ensure removal of personal information prior to returning the device to the finder. If removal of personal information is not possible or cannot be verified without unreasonable expense, the device shall be destroyed in a manner sufficient to eliminate the information, prior to disposal or recycling. The director or the director's agent shall notify the finder that the device was destroyed and disposed of or recycled because personal information could not be removed.

IPSC members discussed whether to specifically name National Institute of Standards and Technology (NIST) Special Publication 800-88 in the proposed amendment. Some members preferred naming the publication, both in regards to sanitation and destroying devices, as it would provide clear direction to agencies. However, it was pointed out that there may be objection from the Attorney General, Legislative Reference Bureau and/or others to including such specificity with regard to a third-party publication (albeit a federal agency). For example, NIST standards go through revisions, which could be problematic is a specific version is written into the law. Ms. Kunimoto stated that she would take the matter back to the AG's office.

The IPSC recessed at 1:30 p.m. due to a fire alarm at the Maui VCC during which occupants were briefly asked to leave. After occupants were allowed back in a couple minutes later, the IPSC returned from recess at 1:32 p.m.

Members continued discussion of what degree of specificity to include in the proposed amendment language. It was noted that the NIST standards and definition of "destroying" devices are relatively simple and consistent, but standards and definition for "sanitizing" devices are voluminous, making it difficult and perhaps ill-advised to attempt to include the latter in statute.

Member Designee Tungol motioned to approve the language, amended with the insertion of NIST Special Publication 800-88, as well as an alternative simply referencing NIST (without the publication), subject to further amendment from the Attorney General. Member Yong seconded the motion. The motion carried with nine members approving and one (Member Levins) abstaining.

VI. Draft Summary Report to the Legislature

Under HRS section 487N-5(d), the IPSC's annual summary report shall include the council's findings, significant trends, and recommendations to protect personal information used by government agencies. Member Designee DeMello noted that the draft summary report, attached to the agenda, included a section for inserting the outcome of the previous agenda item. The section regarding this previous matter will be inserted, subject to amendment by the AG's office, and Exhibit A will be updated to reflect all submissions as of August 28. He also restated the relatively high number of agencies reporting that they are no longer maintaining PI, and that as more agencies submit via the outline form there will be more opportunity to show metrics and greater detail.

Members requested the following revisions:

- Under "Significant Trends"
 - Revise the first paragraph to lead with what is required of agencies, and correct the spelling of "breaches"
 - In the first sentence of the third paragraph, change "is" to "in"
- Under Recommendations to Protect PI Used by Government Agencies"
 - Spell out "personally identifiable information" and omit use of "PII" to avoid confusion with the use of PI (as defined in chapter 487N)
 - Insert the name of "Special Publication 800-88" after the number
 - Insert "(NIST)" after the name, as the entity is commonly known by its acronym
 - Change "sections" to "section"

Member Sherman motioned for the IPSC to approve the IPSC Summary Report, subject to final updates and amendments, and Member Keane seconded the motion. The IPSC passed the motion by unanimous consent.

VII. Internal Handling of Personally Identifiable Information

Proposed Best Practices and Guidelines for Handling Employee Health Information

Members discussed the working list of amendments to procedures with regard to internal handling of personally identifiable information, attached to the agenda. Member Designee DeMello noted that one strategy is to present the final version to DHRD for consideration as an amendment to current procedures.

Chair Nacapuy asked whether the IPSC should be addressing personal devices and mobile devices in particular. The current list did not necessarily address policies for "BYOD" (Bring Your Own Device). Devices handle differently device to device. Members discussed current department-level policies, mobile device management, how to educate employee about risks and best practices. Member Sherman shared that Maui County is working toward its selection of a mobile device management solution in January 2017. Chair Nacapuy shared that the State's enterprise mobile policy is in development by the Enterprise Architecture Working Group. It was suggested that NIST may provide guidance. Some states' policies are that no personally identifiable information is allowed on mobile devices unless justified at the department level for a specific business use.

Since this agenda item, as discussed in previous meetings, had focused on process versus technology, it was determined that the subcommittee should develop a draft memo to DHRD to bring the issue of "process" to closure. The memo should convey:

- IPSC’s desire to work with DHRD to address the issue.
- The practice of attaching doctors’ notes to leave request forms (e.g., state form “G-1”) should cease, with the exception of family and medical leave and/or workers’ compensation records maintained by authorized human resources personnel. Alternatively, it is sufficient for a supervisor to verify that a doctor’s note was presented by the employee (e.g., revised G-1 eSign so that supervisor has option to select “Doctor’s note presented on [date].”
- Best efforts should be undertaken by all departments to ensure only appropriate and authorized staff view and/or handle employee health information. This is typically human resources and direct supervisors, as necessary.
- All employee health information must be secured during transit. When transporting hard-copy materials within the office, said materials must be placed in an envelope labeled with the employee’s name. If transported between office locations, the envelop must be marked “Confidential.”
- The IPSC continues to deliberate on the issue of electronic devices.

The subcommittee will present the memo at next meeting.

Member Yong moved to form a Permitted Interaction Group on the handling PII on mobile devices to address the issue of “technology,” with the group consisting of Members Keane and Yong, Member Designee Tungol, and Mr. Hoang, as well as appropriate staff. Member Designee Ito seconded the motion. The IPSC passed the motion by unanimous consent.

VIII. Good of the Order

Member Designee DeMello noted that future meetings will likely be held in this venue, the Kalanimoku Building basement video conference center. A new invitation email will be sent out to members and member designees with all the 2017 meeting dates.

The next IPSC meeting is scheduled for Wednesday, January 18, 2017, 1 p.m. (The agenda incorrectly list the date of the next meeting as January 18, 2016). It was noted that this is opening day of the Legislature.

IX. Adjournment

Member Sherman moved to adjourn the meeting, and Member Keane seconded the motion. The meeting adjourned at 2:30 p.m.

Respectfully Submitted,

Date

Keith A. DeMello
Senior Communications Manager
Office of Enterprise Technology Services
State of Hawai‘i