Identity Theft Task Force
(Established by Act 140, Session Laws of Hawai`i 2006)
State of Hawai`i
www.state.hi.us/auditor

Minutes of Meeting

The agenda for this meeting was filed with the Office of the Lieutenant Governor, as required by Section 92-7(b), Hawai`i Revised Statutes.

Date: Thursday, January 4, 2007

Time: 9:00 a.m.

Place: State Capitol
415 South Beretania Street
Conference Room 309
Honolulu, Hawai`i

Present: Chair Gary Caulfield, Financial Services Industry
Vice Chair Marvin Dang, Financial Services Industry
Clayton Arinaga, County Police Departments Designee
Craig De Costa, Hawai`i Prosecuting Attorneys Association
Senator Carol Fukunaga, President of the Senate's Designee
Ronald Johnson, United States Attorney for the District of Hawai`i Designee
Representative Jon Riki Karamatsu, Speaker of the House of Representatives Designee
Nathan Kim, The Judiciary
Paul Kosasa, Retail and Small Business Community
David Lassner, University of Hawai`i
Stephen Levins, Director of the Office of Consumer Protection
Tim Lyons, Consumer and Business Organizations
Representative Colleen Meyer, Speaker of the House of Representatives Designee
Carol Pregill, Retail and Small Business Community
Mel Rapozo, Hawai`i State Association of Counties Designee
Robert Takushi, Consumer and Business Organizations
Sharon Wong, Department of Accounting and General Services

Marion M. Higa, State Auditor, Office of the Auditor
Russell Wong, IT Coordinator, Office of the Auditor
Jayna Muraki, Special Projects Coordinator, Office of the Auditor
Sterling Yee, Assistant Auditor, Office of the Auditor
Pat Mukai, Secretary, Office of the Auditor

Jennifer Brooks, Office of Information Practices
Wayne Sasaki, ICSD
Cliff Hirata, ICSD
Richard Shimomura, ICSD
Joanna Markle, Goodsill, Anderson, Quinn & Stifel

Excused: Lt. Andrew Castro, Honolulu Police Department's Criminal Investigation Division
Member, Department of Education
Senator Ron Menor, President of the Senate Designee
Tom Terry, United States Postal Service
Rick Walkinshaw, United States Secret Service Electronic Crimes Unit
Christopher D.W. Young, Department of the Attorney General

Call to Order: Chair Caulfield called the meeting to order at 9:05 a.m. at which time quorum was established

Chair's Report:

Announcements, introductions, correspondence, and additional distribution

Chair Caulfield thanked Representative Karamatsu for providing the refreshments. He reported that letters inviting representatives to make presentations to the task force were sent to several large state agencies and all the mayors' offices. The Bureau of Conveyances will do a presentation in February and the Department of Health in May. We are still waiting for Department of Education and Department of Human Services to reply.

Minutes of previous meeting

Senator Fukunaga moved to approve the minutes of the December 7, 2006 meeting as distributed, seconded by Member Rapozo. It was voted on and unanimously carried to approve the minutes

Informational Briefings:

Department of Accounting and General Services – Information and Communication Services Division

Member Wong introduced the ICSD staff that would assist in the presentation: Richard Shimomura, Assistant Administrator, Clifford Hirata, Production Operations Support Section Supervisor, and Wayne Sasaki, System Services Branch Manager. An outline of the presentation was distributed to the task force members. ICSD's main responsibility is for statewide information processing and telecommunications services and programs. It establishes and operates an overall program for improving government efficiency and effectiveness through telecommunications and information processing technologies. ICSD is the custodian/caretaker of data owned by departments. ICSD processes the data according to the department's rules and policies on the usage of data.

Mr. Shimomura briefed the task force on the state data center. The purpose of the data center is to provide a secure, centralized facility. It houses mainframe and large server systems. Confidential data is processed at the center.

Mr. Sasaki briefed the task force on the two mainframes and the large server systems. One of the mainframes is for the Department of Human Services (DHS) and handles welfare and Medicaid processes. The other systems service the other state departments. Services include payroll, vendor payments, ERS, and unemployment benefits.

ICSD is mainly custodian/caretaker of the data and provides support services, daily backup and off-site storage. On the mainframe side, access is through VPN. Large server systems are accessed through the department's own internal networks.

ICSD uses security software to establish a structure of data elements needed by the departments to manage their security policies. The departments are delegated authority to grant users access permission to their resources based on their operational knowledge and requirements. On the large server system, ICSD provide systems management, and the departments are responsible for network, database, and application security.

On the mainframe, data on disk is not currently encrypted, but the backups are scheduled and sent off-site. On the large server system, all data is backed up and encrypted on tape and the tapes are sent off-site.

Mr. Hirata briefed the task force on physical access, storage, and destruction. The data center has a single point of entry, uses an electronic key system, and has video cameras. Data is destroyed after receipt of proper requests and approvals. Data is either shredded or smashed.

Discussion: Member Takushi asked if computers have been accessed without authorization. Mr. Sasaki said not to their knowledge. ICSD has procedures for handling unauthorized access. ICSD follows an internal process for granting or denying access when a person is hired, separated, or retired. Departments have to rely on their internal policies and procedures for hiring and separation.

Member Levins asked if ICSD has any problems with employees taking laptops with confidential information. Mr. Shimomura replied that ICSD did launch a new project to purchase laptops to allow employees to operate from home to avoid the travel time, but since the Veteran's Administration incident, ICSD has not authorized the use of laptops. They are looking at different types of technology including encryption on the laptops.

Senator Fukunaga stated that during the 2005 session, there was anecdotal information about the loss of laptops with personnel data. The understanding was that ICSD was launching an executive branch-wide initiative to work with all the individual departments, DOE, and UH to establish data security procedures. Mr. Shimomura stated that DAGS received the Legislature's approval to hire three positions, but it took over 1-1/2 years to finalize the position descriptions. DAGS is now in recruitment for three cyber security experts to assist other departments with their policies and procedures.

Member Takushi asked if ICSD has a plan in the event of a major disaster. Mr. Shimomura replied that for the last three years the department has been trying to get a $2.7 million appropriation to lease an alternate data center.

Chair Caulfield asked if there is a statewide policy being developed or under consideration about access so everything is standardized. Mr. Shimomura answered that policies are available on the ICSD website, but they need to be updated. Mr. Sasaki stated that there is a standard process the departments go through for mainframe access using the security software and each department has a security officer. The departments know their own operations/applications the best. ICSD doesn't know the department's applications. Chair Caulfield asked if ICSD monitors file access and logs. Mr. Sasaki stated that ICSD monitors logs for violations. If a violation, it would appear in the security log and the department is notified.

Chair Caulfield asked if there are standard policies or best practices for security access for departments and if a central person knows what the departments are doing. Mr. Sasaki said no central person knows the whole state, but the methodology is standardized.

Chair Caulfield asked if ICSD employees have access from their home computers. Mr. Shimomura said not to their knowledge. Chair Caulfield asked if the governance committee is discussing redaction and ways of minimizing public access or exposure to social security numbers. Mr. Shimomura said this is a concern and they are constantly working on it. The governance committee is looking at this.

Senator Fukunaga stated that private sector is held to a high standard of personal information security and severe penalties apply for any breaches. It is important that government agencies be held accountable to the same standards. In testimony, they have heard that records at Family Court and the Bureau of Conveyances contain personal information and are routinely scanned by external parties such as collection agencies, title companies, etc. The agencies pointed out it would be quite expensive and very difficult to tackle the problem. One of the reasons for this task force is to see how we could work with government agencies.

Chair Caulfield thanked ICSD for their presentation.

Office of Information Practices – Presentation on the Uniform Information Practices Act:

Office of Information Practices

Jennifer Brooks from the Office of Information Practices briefed the task force on the Uniform Information Practices Act (UIPA). Ms. Brooks distributed a booklet, "The Uniform Information Practices Act – Hawai`i's Open Records Law." For most government records, any information that government maintains in tangible form, there's a presumption that they are public, but there are exceptions. The privacy exception to disclosure would cover social security numbers, financial account information, home address, home phone number, mother's maiden name, date of birth, all items that would raise identity theft concerns. These exceptions are not mandatory, however, and the agency has discretion.

Section 92F-12 lists categories of records that are required to be public. Records listed in section 92F-12 are required to be public and exceptions do not apply unless an exception is written specifically into the section.

Discussion: Chair Caulfield asked if OIP received any complaints alleging possible violation by agencies and if they received any complaints relating to identity theft. Ms. Brooks responded that most of the complaints they receive involve an agency denying access to records or an agency failing to respond to a request for records. OIP only gets a couple of complaints a year alleging violation of privacy, and there's very little OIP can do in those situations.

Auditor's Report

Jeffrey Loo of J.W. Loo & Associates, consultant, reported on some of his work. Personal information questionnaires were sent to four counties and state agencies, including the UH and the Judiciary. He included questions regarding their awareness and readiness to comply with the ID theft laws and the social security number act, and whether they have developed policies to conform with those acts. A follow-up notice will be sent to the agencies to remind them of the deadline is January 31st.

He has also started a survey of other jurisdictions to identify best practices. Last year's task force report indicated 33 states have ID theft laws. Now, it appears that all states have ID theft laws in place. He is focusing on the policies and practices of states that include state agencies in their compliance requirements.

California seems to be the model for many other states. They have an extensive framework of laws and created an Office of Privacy Protection in 2000. The office serves both the state and consumers. It assists individuals with identity theft and privacy concerns and promotes consumer education. It is also involved in coordinating local, state, and federal law enforcement and recommends policies and practices to protect individual privacy.

Some of the Office of Privacy Protection's 2005-2006 highlights:

- Worked on consumer education materials.
- Conducted workshops and seminars for consumer and community groups as well as business, government, and professional groups. An event was held in Los Angeles with 1,000 attendees, "Teaming Up Against Identity Theft-A Summit on Solutions," which created some best practices materials.
- Participated in advisory groups.
- Hotline where consumers can call when they have complaints or questions.
- California Business Privacy Handbook – provides guidance that follows some of their privacy and ID theft laws to help guide businesses in conforming with those laws.
- Recommended Practices on Notice of Security Breach – a step-by-step checklist in terms of what to do if you have a security breach involving personal information.

California practices on information sharing, disclosures, and privacy policies and laws

include the following:

- State agencies are required to create a log when they share or disclose information for non law enforcement purposes.
- Recommended Practices for Protecting the Confidentiality of Social Security Numbers – a document that includes a statement of best practices.
- Model Policy on Access to Court Records of the Justice Management Institute and the National Center for State Courts.
- Protecting Privacy in State Government – a basic tutorial on managing personal information, do's and don'ts of how to handle and prevent unauthorized access.
- Notification of Security Breach of Personal Information – there is a breach response call center FAQ sheet; a to-do list when you have a breach.
- Credit Card Address Change – a law that requires some validation/confirmation when a credit card issuer receives an application that's different than the one on the application form. A common way to steal an ID is to get an application out of someone's mailbox, fill it out, and change the address.
- Employment of Offenders – prisoners are not allowed to access personal information.
- Information Practices Act of 1977 – basic practices and requirements for agencies. Agencies should only maintain and collect information that are relevant and necessary to accomplish the purpose.
- Information Sharing Disclosure – this creates an affirmative requirement on a state agency to respond to a consumer who wants to know who their information was given to. It allows the agency to respond by creating a list of categories of personal information disclosure to companies for marketing purposes or allows them to provide a privacy statement and giving the customer a cost-free opportunity to opt-out of information sharing.
- State Agency Privacy Policies – requires state agencies to create privacy policies and to designate an employee to be responsible for the policy.
- Penal Code Sections 530.5 – 530.8 – requires law enforcement agencies in the victim's area to take a police report.
- Personal Information Collected on the Internet from Government Agencies – when agencies collect personal information electronically, they must have a notice on that website and obtain written consent before sharing information with third parties.

Interim Report: Mr. Wong reported that an interim report was circulated to all members via email. It summarizes the work of the task force so far. Vice Chair Dang moved to adopt the report that was circulated, seconded by Senator Fukunaga. It was voted unanimously to adopt the report.

Investigative Working Groups – Reports: Member Levins indicated that his sub-task forces created to research best practices and issues relating to compliance issues will meet on Monday, January 8th at 9:00 in Room 325.

Meeting Schedule:	Chair Caulfield stated that the first Thursday of every month seems to be the best date for most members.	
	Chair Caulfield moved to adjourn the meeting, seconded by Member Rapozo. It was voted unanimously to adjourn the meeting.	
Next Meeting:	date:	Thursday, February 1, 2007
	time:	9:00 a.m.
	address:	to be determined
Adjournment:	With no further business to discuss, the Chair adjourned the meeting at 10:24 a.m.	

Reviewed and approved by:

Russell Wong
IT Coordinator

February 1, 2007

[ ] Approved as circulated.

[X] Approved with corrections.

ID Theft/010407