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, June 7, 2007

Time: 9:04 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
Lt. Andrew Castro, Honolulu Police Department's Criminal Investigation Division
Fay Ikei, Department of Education
Senator Carol Fukunaga, President of the Senate's Designee
Representative Jon Riki Karamatsu, Speaker of the House of Representatives Designee
Paul Kosasa, Retail and Small Business Community
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
Robert Takushi, Consumer and Business Organizations
Christopher D.W. Young, Department of the Attorney General

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
Albert Vargas, Analyst, Office of the Auditor
Pat Mukai, Secretary, Office of the Auditor

Jeffrey Loo, J.W. Loo & Associates
Colleen Schrandt, Legislative Auditor, County of Hawai`i
Maxine Pacheco, County Clerk, County of Hawai`i
Rod Moriyama, Department of Education
Mel Decasa, Department of Education
Lim Yong, Department of Human Services
James Castro, Department of Human Services
Jodi Ito, University of Hawai`i
Wayne Yoshioka, Hawai`i Public Radio
Joanna Markle, Goodsill Anderson Quinn & Stifel

Excused: Craig De Costa, Hawai`i Prosecuting Attorneys Association
Ronald Johnson, United States Attorney for the District of Hawai`i Designee
Nathan Kim, The Judiciary

David Lassner, University of Hawai`i
Senator Ron Menor, President of the Senate Designee
Mel Rapozo, Hawai`i State Association of Counties Designee
Tom Terry, United States Postal Service
Rick Walkinshaw, United States Secret Service Electronic Crimes Unit
Sharon Wong, Department of Accounting and General Services

Call to Order: Chair Caulfield called the meeting to order at 9:04 a.m. at which time quorum was established.

Chair's Report:

Announcements, introductions, correspondence, and additional distribution

Chair announced that a presentation by Symantec Corporation will be held on Thursday, June 14, 2007, at 9:00 a.m. at the State Capitol, Conference Room 309. There will be a second session at 1:00 p.m.

Chair also announced that he received a letter from the Consumer Data Industry Association (CDIA), which represents 400 data providers, asking to make a presentation to the Task Force at the August 2 meeting.

Minutes of previous meeting

Member Young moved to approve the minutes. Vice Chair Dang seconded. It was voted on and unanimously carried to approve the minutes.

Informational Briefings/ Discussion:

County of Hawai`i, Legislative Auditor's Office and County Clerk

Colleen Schrandt, Legislative Auditor and Maxine Pacheco, Information Security Officer, Office of the County Clerk, County of Hawai`i, briefed the task force on the records kept by the Hawai`i County legislative branch.

The Hawai`i County Clerk's office maintains 54 types of records for employees that contain personal information including full names social security numbers. The Elections Division maintains and stores records of all voters, totaling an estimated 100,000 to 500,000 records. Personal information is shared among government and non-government agencies.

The office is updating policies and procedures for collecting, handling, accessing, safeguarding, protecting, and disposing of confidential information. Mandatory informational training workshops are provided to employees regarding confidentiality and handling of personal information. There has been no known unauthorized access to personal information.

Physical security includes monitoring the issuance of office key(s) and locking computers, office desks, and filing cabinets. IT solutions include county internet and email policies, computer access request, secure fiber network, etc. Plans to protect electronic information include education and training on how to encrypt/decrypt files with personal information and how to safeguard personal information stored on laptops, CDs and flash drives. They will be incorporating hard disk encryption on all laptops, as well as biometric security (fingerprint readers). Software will be addressed by tightening network security with the new Windows 2003 server.

The County Clerk-Council's Office has drafted an information security and privacy plan to comply with the requirements of Chapter 487J, HRS (Social security number protection), and 487R (Destruction of personal information records). Although this draft plan is generalized and not specific, a subgroup will be addressing specific areas. The draft should be finalized in the next six months.

Chair Caulfield asked whether it would help their agency if they were given a best practice

model. Ms. Schrandt responded yes.

City and County of Honolulu

Keith Rollman, Senior Advisor, Department of Information Technology, City and County of Honolulu (City) briefed the task force.

The City stores millions of records and serves a number of constituencies including the State of Hawai'i, Honolulu Police Department, and the Judiciary. As of December 26, 2006, the City and County has implemented an interim program to comply with HRS Chapters 487J, 487N, and 487R to protect individuals from identity theft. The County is in the process of transitioning to a new generation of software and hardware.

Personnel information is stored by both electronic means and paper-based forms. Paper-based forms are used to collect personnel information for federal and state tax forms, designation of beneficiary forms, deferred compensation forms, payroll forms, etc. Each department handles the security, maintenance, and disposal of their paper-based forms following the City's policy on protection of personnel information.

Since November 2004, social security numbers have not been used as employee ID numbers. Internal forms that required social security numbers have been converted to employee ID numbers.

Two of the City's electronic repositories, the CHRMS (City Human Resource Management System) and the CIFIS (Computerized Integrated Financial Information System) which contain personnel and vendor information respectively are being changed. Various areas and systems used within the City such as the Driver Training File, Liquor Commission, Worker's Compensation System, Police Firearm System, and Police ID System, HOKU (prosecuting attorney case tracking system), Driver's Licensing System, Voter Registration system, etc. all contain personal information.

Policies developed by the Department of Human Resources are in place that cover issues such as agency roles and responsibilities, disclosure authority, protection of paper records, special precautions for social security numbers, breach notifications, disposal of information, and training programs for those who handle confidential information.

Member Young noted that the interim program policy is a comprehensive plan that addresses personnel information and inquired whether the City had a separate document that covers personal information. Mr. Rollman responded that they have a separate section of their internet policy that deals with network security and web services on transactional requirements. Member Young asked whether the internet policy deals with personal information being kept and protection of social security numbers. Mr. Rollman replied that their policy specifically is written in response to HRS, Chapter 487.

Member Young also inquired about general information collected from the public. Mr. Rollman responded that it is out of the jurisdiction of the IT department, as it is all handled at the departmental level and there are standards to follow.

Member Levins noted that effective July 1, 2007, individuals do not have to be victims of identity theft to freeze their credit reports. He suggested that the City revise their form letter on security breach. Member Levins also suggested that the City confer with Corporation Counsel at any time there is a security breach due to the different levels of breaches and in certain instances, the form letter may not be appropriate.

Member Takushi asked if the City consolidated its policies and procedures into one department that is responsible for all other departments. Mr. Rollman replied that the paper files stay within the departments and disposal of those documents are their

responsibility. The City has policies on destruction of documents. All documents are shredded by employees at their workstation or by professional companies.

Department of Human Services – Med-QUEST Division

Lim Yong, HIPAA Project Manager, and James Castro, IT Security Manager, Department of Human Services, Med-QUEST Division, briefed the task force.

The Department of Human Services (DHS), Med-QUEST Division, (MQD) provides financial and medical assistance, vocational rehabilitation, and public housing to 250,000 lower income Hawai`i residents annually. DHS-MQD also oversees the Office of Youth Services and Child and Adult Services.

DHS-MQD maintains over 2,800 employee records. DHS-MQD collects and stores client information such as names, social security numbers, and bank account numbers as required by law to fulfill the program's mission. However, DHS-MQD does not collect access codes or passwords that access an individual's financial account.

Personal information is made available to third parties when required by Federal or State laws; required in MOA/MOU as permitted under applicable laws; authorized by the individual; or required in contractual obligations as permitted under applicable law.

Current policies and practices are in place for internal and external access of personal information. The Deputy Director is responsible for overall policy compliance with privacy and security of confidential information.

Solutions are in place to protect personal information that include periodic risk assessment and remediation, periodic audits as required by DHS policy, and facility upgrades such as door locks, privacy screens for workstation monitors. DHS-MQD also plans to implement biometric and multi-factor authentication and to scrub computer hard drives that need to be replaced or to be returned to the vendor with DOD certified scrubbing software.

Training is provided to staff regarding the confidentiality and handling of personal information. Funding to implement security technologies, resources to implement hardware and software, and resources to audit and monitor compliance are DHS' most critical need to ensure security of personal information.

There has been no unauthorized access to personal information in 2006 and none to their knowledge over the past several years.

DHS has taken steps to comply with the requirements of HRS Chapters 487J, 487N and 487R. DHS also has policy guidelines on physical security and technical safeguards to protect personal information.

Various federal laws require specific retention periods before disposal of files. DHS-MQD also adheres to the DAGS inventory and disposal of government record policies. All paper-based forms are shredded internally or by a private contractor. All computer hard drives are scrubbed or crushed before disposal.

Member Takushi asked what solutions the state could offer in general to address problems with protecting personal information. Mr. Yong replied that there are so many records that it is difficult to manage. A document imaging solution and statewide email encryption are possibilities.

Vice Chair Dang asked whether the department has communicated with other state departments regarding personal information policies. Mr. Yong replied that they do

contact other departments and discuss the issues. They are also required to follow federal guidelines.

Member Young stated the DHS-MQD is excluded from some of the provisions of HIPAA regarding personal information, however, he asked if there were specific policies related to non-HIPAA records. Mr. Yong said there are specific guidelines that are more stringent depending on the regulation.

Representative Meyer asked how DHS-MQD keeps an employee from copying, taking, and sharing information with others. Mr. Yong replied that they are currently implementing procedures on viewing information. These procedures involve keeping a record of individuals viewing particular information. However, this will not prevent an individual from viewing information. The records are kept on the average for 90 days up to a year. Email records are kept longer.

Member Young stated that 90 days is too short and recommended that their records be kept longer. He also inquired whether DHS-MQD would need help in funding. Mr. Yong replied "yes."

Department of Education

Rodney Moriyama, Assistant Superintendent for Technology and Mel Decasa, Project Manager, Department of Education, briefed the task force.

The Department of Education (DOE) is the 10th largest school district in the country. There are 285 schools, 179,000 students, 20,552 regular employees, and 23,149 casual/part-time employees.

The major identity theft challenge for the DOE is decentralization of all paperwork and hiring practices. The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. DOE follows FERPA as guideline for student confidentiality.

As an operational policy, DOE restricts against electronic input of social security numbers for employees and students in the Student Information Systems. Other inputted personal information for both students and employees includes: name, date of birth, residence address, and phone numbers.

The department is just beginning to centralize the student information system and is implementing a new human resource system. Four years ago, the department started to do electronic document management. So far, 70 million documents have been scanned.

DOE electronic systems must have the ability to maintain both active and inactive records containing personal information. The payroll system has allowances for 1 million transaction records. The personnel system has allowances for 100,000 transaction records. The student information system has allowances for 300,000 transaction records.

Employee personal information is made available to third parties for background checks, teacher certification, and federal compliances for payroll. Employee social security numbers are used internally for payroll and personnel, and externally for employee verification and certification.

There is no centralized authority to mandate and monitor compliance. There have been at least two incidents of unauthorized access. In December 2005, six PCs were stolen from the payroll department, and in February 2007, personal checks from eighteen schools were taken from an armored car.

The payroll and accounting offices have written policies regarding nondisclosure of employees' social security numbers. Operational policy restricts against use of student social security numbers. The DOE utilizes FERPA, HIPAA, IDEA, Chapter 34 (HAR), as their current policies and practices related to internal and external access and security.

The disposal of personal and confidential information is decentralized and left up to the discretion of offices and schools. All personally identifiable hardcopies are shredded.

The DOE has identified at state level, forms and reports that include personal information; surveyed schools and offices on estimated volume of documents and digital records; and formed formal taskforce with project manager to implement action plan to be in compliance. IT based security solutions are currently in place.

Training is available for internet access and for security access regarding the student information system, comprehensive student support system, financial management system, lotus notes, time and attendance system, and compliance training for administration.

The agency's most critical need to assure security of personal information involves training and awareness, centralized focal point for security, accountability/monitoring (signed document annually reviewed), and standardized disposal and destruction of information.

Member Takushi asked with the inconsistencies and lack of standards, how is the DOE going to handle this, how much money is it going to cost, and whether the DOE has identified at least, a process of priorities in which to address in terms of potential risks that is out there for damage. Is there a priority list of where the most risk is? Is there a priority list? Mr. Moriyama replied that the number one priority is to raise the level of awareness so everyone is aware of the concern.

Member Young inquired about student social security numbers and where they are stored. Mr. Moriyama stated that they do not keep student social security numbers but they do have employees' social security numbers. Member Young further asked how the DOE verifies students. Mr. Moriyama responded that they have registration policies for students.

Representative Meyer asked whether there were hardcopies kept at the schools and if the schools keep payroll information. Mr. Moriyama responded that the schools keep social security numbers, and the department has very tight security on student information and leave records, and especially health-related and special education.

Member Young asked whether the "tight security" means that computer files are encrypted and locked in file cabinets. Mr. Moriyama confirmed that tight security means locked filing cabinets. Some schools have vaults for their special education student records, but not every school has a vault. Some have locked cabinets. Some schools keep their records in the principal's office under lock and key. The level of security is not consistent. Each school has its own way of managing files.

Auditor's Report

Jeffrey Loo of J.W. Loo & Associates, consultant, gave a status report and preliminary findings to the task force on the following:

1. Define personal information – The compilation and research is completed and he is in the process of preparing the report.
2. Identifying Best Practices – The compilation of the scan of all the states' statutory is completed.
3. Perform Risk Assessment of State/County Agencies – About 100 surveys were

sent out to state and county level agencies. However, in response, there were about 300 surveys completed as some lower divisions and branches completed the surveys. He is in the process of completing the review.

4. Review Current Social Security Number Practices – In the process of completing the review.

Mr. Loo reported the following:

Definition
California's definition is similar to what we have as our definition of personal information on the security breach and notification side, however their definition on the criminal side is different. Their definition is basically a name combined with certain specific identifiers. The specific identifiers are social security numbers, driver's license and then they go into financial-type related information and medical information.

Identity Theft Components
Identity Theft Components includes logos, symbols, and trademarks-business identity. Across the 50 states references to social security numbers, driver's license, birthdates, etc. are very common. Government types of identifiers include health insurance identification numbers, demand deposit account number, and electronic identification number for routing codes. Other logos, symbols, and trademarks may include telephone numbers, telecommunication identifying number, access device number, Medicaid or food stamp account number, medical records, student identification number, and military identification number.

Information Breach/Notification
Many states have followed the structure California has done for personal information. Some states apply definition only when personal information is unencrypted or unredacted. Other states, for example Nebraska, focus on electronic commerce.

Overview of Best Practices
In general, California is the only state in the union that has created a specific office on privacy protection. They have a broad assignment that includes assisting individuals and providing privacy education.

Reduce Exposure and Prevention
California has posted recommended practices for protecting the confidentiality of social security numbers on their website. California enacted specific legislation to limit the scope of information collected and maintained by agencies.

Education
California's website includes a section directed toward state employees in terms of creating awareness. They developed bilingual consumer education materials and have conducted workshops for consumer and business groups.

Safeguards – what policies or technical measures to protect information.
California requires agencies, on all documents collected, to include a notice with the agency contact, authority under which the information is being collected or maintained, whether submission of the personal information is mandatory or voluntary, the consequences for not providing the requested information, the purpose of the collection, and the individual's right to access the information.

Mitigation - what to do after a breach occurs and how to reduce the impact on the consumers or agencies.
Many states require notification in case of security breach. Some limit requirement to incidents involving suspicion that there may be harm to individuals.

2007 Legislation

Mr. Wong briefly described the handouts distributed to task force members:

- Summary of March sub-task force meeting for those who were not able to attend.
- Copy of Illinois' Department of Financial and Professional Regulation webpage regarding a breach.
- OMB memorandum regarding Safeguarding Against and Responding to the Breach of Personally Identifiable Information. It requires agencies to develop a breach notification policy.
- A letter, including a set of questions, from the House Committee on Homeland Security to the Department of Homeland Security regarding information system security.
- Handout – study from Dartmouth College regarding peer-to-peer networks and inadvertent disclosures of personal information on those networks.
- There are a number of bill in Congress that deal with identity theft. One example is S.1178, which, if enacted into law, would pre-empt any state laws.
- At the state level, House Bill 1004 is pending the governor's action. This is the bill that would appropriate $100,000 for the task force.
- House Resolution 198 discusses notary public and the process they currently use and it asks the task force to look at the process.
- House Bill 1612, pending governor's action, would allow any resident to put a security freeze on their credit report.

Investigative Working Groups – Reports:

Member Young reported that their working group reviewed Member Lassner's report regarding the understanding and protecting against identity theft. The subcommittee agreed and disagreed with some of the information. Their written comments will be submitted at the next task force meeting.

Member Levins reported that their working group received information from various members and will be preparing a one-page document on best practices for businesses.

Meeting Schedule:

Chair Caulfield asked the auditor's office to lay out some tentative dates in order for the task force to meet its mandate of submitting a report to the 2008 Legislature. The following is a tentative schedule of meetings for the task force for the remainder of this year:

July 12, 2007
August 2, 2007 – Presentation from the Governor's Office and the Consumer Data Industry Association, and report outline will be presented.
September 6, 2007 – Draft findings are presented from the Investigative Working Groups
September 27, 2007
October 25, 2007 – Decision making on any proposed legislation.
November 15, 2007 – Approve draft report.
December 6, 2007 – Final Meeting- approve final report.

The final report is due to the Legislature on December 27, 2007.

The task force members were asked to check their calendars on their availability regarding the tentative meeting dates. Some of the meeting dates were moved from the first Thursdays of the month. If the task force stays on track according to the dates above, the report should be submitted on time.

<u>Agenda item VI. (b) – Creation of an additional working group to meet with the consultant and auditor staff to provide guidance as needed</u>.
Should the Governor signed the House Bill 1004, the task force would need to select a consultant to complete phase two of the report. Jeffrey Loo is completing phase one,

including the best practices research. Chair Caulfield proposed the creation of a third working group to meet regularly to assist the auditor's staff and the consultant. This would not be a decision-making committee and it cannot exceed more than 11-12 members. Chair Caulfield volunteered to chair this sub-group. He recommended that the two chairs of the investigative working groups be a part of the sub-group. He also recommended that this group be comprised of one or two representatives from the Legislature, private sector, and law enforcement. Senator Fukunaga and Representative Karamatsu will be members representing the Legislature and both Vice Chair Dang and Member Takushi volunteered to be a part of this sub-group as members from the private sector.

Vice Chair Dang moved to set up a third working group to meet with the consultant and the auditor's staff to provide guidance as needed in preparing the report, seconded by Member Takushi. It was voted unanimously to approve this sub-group.

Other: Vice Chair Dang stated the task force should address House Resolution 198 in terms of deciding what course of action the task force might want to take on this. At a minimum, there should be a presentation by the Attorney General's Office (AG) and a public organization regarding this matter. It was his understanding that this resolution was originated by Representative Tokioka based on a situation that is currently in the newspaper in which an individual may have substituted pages in a notarized document to commit fraud. The resolution requests that the AG's office and the task force identify ways in which the process of notarizing documents can be improved to reduce identity theft, by requiring the notary's seal to be placed over a succinct phrase identifying the nature of the document and the underlying transaction.

Member Young stated that the responsibility of the notary does fall within the AG's office. In order for a notary to certify something, some form of identification, such as a driver's license, state ID, or passport, is required. To prevent fraud from notarized documents seems to be outside the scope of what notarized certification process is, or what a notary does when he/she notarizes a document. Member Young stated that he can request a representative from the notary office do a presentation on their procedures and processes. Chair Caulfield indicated the presentation can be scheduled for the July 12th meeting.

Adjournment: Member Young moved to adjourn the meeting, seconded by Member Takushi. It was voted on and unanimously approved to adjourn the meeting.

With no further business, the Chair adjourned the meeting at 11:43 a.m.

Next Meeting:
date: Thursday, July 12, 2007
time: 9:00 a.m.
address: to be determined

Reviewed and approved by:

Russell Wong
IT Coordinator

June 25, 2007

[ ] Approved as circulated.

[…..] Approved with corrections; see minutes of _____ meeting.