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, September 6, 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
Lt. Andrew Castro, Honolulu Police Department's Criminal Investigation Division
Senator Carol Fukunaga, President of the Senate's Designee
Fay Ikei, Department of Education
Jodi Ito, University of Hawai`i
Nathan Kim, The Judiciary
Stephen Levins, Director of the Office of Consumer Protection
Tim Lyons, Consumer and Business Organizations
Senator Ron Menor, President of the Senate Designee
Representative Colleen Meyer, Speaker of the House of Representatives Designee
Carol Pregill, Retail and Small Business Community
Robert Takushi, Consumer and Business Organizations
Tom Terry, United States Postal Service
Sharon Wong, Department of Accounting and General Services
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 Oshiro, Special Projects Coordinator, Office of the Auditor
Albert Vargas, Analyst, Office of the Auditor
Pat Mukai, Secretary, Office of the Auditor

Jeffrey Loo, J.W. Loo & Associates
Joanna Markle, Goodsill Anderson Quinn & Stifel
Kalbert Young, County of Maui, Director of Finance
Lito Vila, County of Maui, Division Administrator, Division of Motor Vehicle and Licensing
Scott Teruya, County of Maui, Assistant Division Administrator, Real Property Tax Division

Excused/ Absent: Craig De Costa, Hawai`i Prosecuting Attorneys Association
Representative Jon Riki Karamatsu, Speaker of the House of Representatives Designee
Paul Kosasa, Retail and Small Business Community
Mel Rapozo, Hawai`i State Association of Counties Designee
Rick Walkinshaw, United States Secret Service Electronic Crimes Unit
Ronald Johnson, United States Attorney for the District of Hawai'i Designee

Call to Order: Chair Caulfield called the meeting to order at 9:07 a.m. at which time quorum was established.

Chair's Report:

Announcements, introductions, correspondence, and additional distribution

Chair Caulfield announced that the September 27, 2007 meeting has been cancelled and the October 25, 2007 meeting will be moved up possibly a week or two. The Auditor's Office will be polling the members on their availability.

Minutes of previous meeting

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

Informational Briefings/ Discussion:

County of Maui

Kalbert Young, County of Maui, Director of Finance
Lito Vila, County of Maui, Division Administrator, Division of Motor Vehicles and Licensing
Scott Teruya, County of Maui, Assistant Division Administrator, Real Property Tax Division

Mr. Young briefed the task force on the records kept by the 17 Executive Branch departments and agencies.

The County of Maui has approximately 2,300 full and part-time employees. The various types of records with varying degrees of personal information are maintained at the divisional, departmental, and countywide levels.

The County collects and stores records of all employees, businesses, and taxpayers' personal information. Employee records include human resource/service files, personnel files, applications, tax records, and payroll records. Business records include procurement files, contractor files, tax records, licensing records, and service applications. Taxpayer records include records maintained by the Departments of Finance (driver's license records, vehicle registration, real property information, tax records), Housing and Human Concerns (applications for aid and services), Public Works (home refuse collections and landfill customers), and Water (applications for service). All departments also maintain duplicative files pertaining to their employees, businesses, and contractors that perform work for their particular department.

There are over a million records that contain personal information maintained by the following departments:

Finance:

- DMVL = over 1,000,000 records with combination of social security number, name, address, drivers license number.
- Real Property Tax – this division maintains over 500,000 records with names, addresses, and social security number combinations with payment instruments.
- Accounts Division – over 1,000,000 records with combination of names, addresses, and social security numbers with payment instruments.
- Procurement – over 100,000 records with names and addresses.

Police:

- Over 1,000,000 records with names, addresses, and social security numbers.
- Records related to employees, arrest files, incident reports, etc.

Liquor Control:

- About 1,000 records with applicant names, businesses, addresses, and social security numbers.

Prosecuting Attorney:

- Approximately 100,000 records with names, addresses and social security numbers combination. This information routinely required to and from the Judiciary.

Water Department:

- Over 50,000 records attributed to water meter applications. These records contain names, addresses, social security numbers, and account numbers.

Housing and Human Concerns:

- Over 25,000 records with names, addresses, social security numbers, tax information. These include information from landlords, tenants, immigration, and Federal Housing Assistance applications.

Personnel Services:

- Over 500,000 records with combination of names, addresses, and social security numbers.

Public Works:

- Over 10,000 records with combination of names, addresses, and social security numbers.

Management Information Systems (MIS):

- Maintains the county server, database and all IT systems. They represent the collaborative, entire record-base for every single department.

Every department has restrictions on allowing the distribution of any information to public and private third parties. The County has arrangements to share or exchange information with other state, federal, and county agencies, law enforcement, and judiciary.

Currently, there are no formal policies or guidelines on a countywide basis that govern the distribution or access to personal information. The county administration is in the process of looking at avenues to establish formal policies in the following areas: Countywide IT, Employee Handbook, and Standard Operating Guidelines and Procedures. Departments have internal operating guidelines and procedures that limit or provide employees with direction limiting internal and external access to information.

The IT Security Policy does limit access to any data stored on the county server and network maintained by the MIS department. Departments practice redaction of records when communicating within other county departments or to external parties.

Departments are responsible for securing their own departmental files, records and systems that exist outside of, or are not on county platforms. Files are routinely stored and locked on-site and off-site with access restricted to certain staff.

The County does not have an overall manager responsible for access and security within the agency. The Countywide IT security is within the purview and authority of the Department of Management-Management Information Systems Division (MIS). Currently, the policy for information security is governed through the MIS departmental policies applied on a countywide basis.

There have been no reports of any unauthorized access to personal information within the countywide IT system or within any departmental level records or files.

The various departments provide training to employees on methods and practices to safeguard confidentiality of personal information. However, there is no standardized or formal countywide training program and no established formal countywide policy or guideline for safeguarding personal information.

The departments report that the following are needed to improve security of personal information:

- Update the records retention policy. The County's current records retention policy dates back to the 1990s.
- Add more resources dedicated to IT security.
- Additional funding for security measures (electronic and physical).
- Additional funding for security consultant/expertise.

- Additional staff and resources. There is no dedicated information security officer.

The departments are in the process of assessing the impact of Chapter 487 on operations. The prosecutors are evaluating how filing of court documents complies with Chapter 487. The payroll system is being modified to prevent displaying of social security number to those who have access. Tax records and all correspondences are redacted for social security numbers before distribution.

Physical security is in place that limits access to records and information. IT security limits access on the countywide system. Upgrades to the IT system will restrict the depth of personal information available for viewing and allow more control over printing of personal information. A security assessment was conducted in 2006. Annual follow up assessments and reviews are planned.

Physical records are disposed of by using departmental shredders and by utilizing destruction contractors. The destruction of electronic records is handled by purging the records to archive. The system currently maintains all records placed onto the IT system. The records retention policy does not address destruction of electronic data such as emails or other files stored on the server.

Member Takushi asked whether electronic records are kept forever. Mr. Young noted that Maui county has not updated its records retention policy since the early 1990s, and the policy does not address electronic records. Departments are advised not to destroy any records unless there is a policy allowing destruction.

Member Wong asked for more information about the county's security consultant hired in 2006. Mr. Young stated that the consultant is not on contract any more. Although the work did entail some levels of personal and information data storage security, it was largely physical security. The consultant assessed security in areas accessible to personnel, public areas, and areas in which records are stored and looked at IT vulnerability.

Mr. Young also explained that the county building has limited physical security. The finance department has a locked security door requiring a badge to enter. Access is granted to employees who do business in the finance department. However, other floors including the Mayor's office and the County Council have no security.

Member Young asked how the county defines personal information? Mr. Young replied that the personal information is any individual component that would include name, address, social security number, and any identifier to that person or individual. For purposes of this presentation, they used any combination of two elements. Member Young asked if all county employees are required to sign a user agreement with regard to accessing the county's computer system as well as use of personal information. Mr. Young replied that employees are required to sign an agreement on the use of the county computer system and abide by the policies established for IT and computer use. However, there is nothing similar to cover use and distribution of personal information. Mr. Young stated that they are planning a countywide policy to address personal information security.

With respect to personal information that is printed, Mr. Vila stated that his division contracts with a private shredding vendor to shred all confidential information on-site weekly. Employees are instructed, by memorandum, to put all confidential information into a box for shredding. The Prosecutor's office and the Real Property Division also utilize a vendor to shred their documents on-site.

Member Young asked if there is a policy on destruction of hardware. Mr. Young stated

that the MIS division is accountable for all IT equipment for every single department. The MIS division maintains and inventories all the equipment. The division's policy is to physically destroy all hard drives.

Member Lyons asked why a social security number is required to charge a fee to pick up trash. Mr. Young did not know why this requirement existed, but many forms were created a long time ago and have not been revised.

Mr. Loo stated that the county reports that the agencies do not disclose, trade, or sell data to third parties. Other agencies, state and county, report they do transmit to vendors such as LexisNexis, national reporting agencies, and fire departments, etc. He asked if the county does any of that. Mr. Young replied that they would disclose information and personal data to government agencies such as EUTF, ERS, and pseudo-government entities; however, the county does not transmit or sell information to private entities.

Chair Caulfield asked if going forward the county will have one coordinator to develop a plan and make sure everyone moves in the right direction. Mr. Young said he could not answer that. A chief information officer, or someone in that position, would not be located in the finance department. He is not aware of any plans to do this, though the managing director has said this is a likely direction for the county.

Chair Caulfield thanked the County of Maui for their presentation.

Auditor's Report:

The Auditor's Office has engaged the same consultant for the next phase.

Consultant's Report

Jeffrey Loo of J.W. Loo and Associates, consultant, briefed the task force on the following:

Mr. Loo reported that he has completed the sections defining personal information and identifying best practices. He has received some feedback from some of the members and will be incorporating it into the final draft. There are two outstanding sections: 1) performing the risk assessment of state and county agencies, and 2) reviewing current social security number practices. Mr. Loo stated that he has begun drafting these sections.

Phase II of the work consists of three sections: 1) Assess the future growth/decline in document records containing personal information, looking at current volume as well as the projected growth and decline as reported in the survey that was conducted in Phase I. 2) Examine the practicability of mandatory redaction of personal information. Mr. Loo has projected a couple of activities, one is to revisit the information already collected to assess other jurisdictions' approaches and solutions to mandatory redaction of personal information, and looking at industry standards and tools. Mr. Loo also proposes to conduct four focused interviews with agencies for information on their particular issues and potential barriers to mandatory redaction requirements. 3) Identify solutions related to the protection of social security numbers; assess the range and scope of social security numbers used and the sale, lease, trade, rental, or disclosure to third parties.

In terms of schedule, Mr. Loo is looking at submitting a draft for Phase I at the November 13th meeting that would ensure that the task force has time to review recommendations and submit the final report to the Legislature for the upcoming session. Phase II should be on the same schedule.

Senator Fukunaga stated that in terms of possible solutions with respect to mandatory redaction, she brought some materials from the NCSL conference. Apparently, there is a growing industry trying to provide solutions to this problem. There are a number of vendors developing electronic redaction solutions. Mr. Loo responded that he is aware of some of the vendors, however, he is not sure right now if it can be incorporated into the

report. He did follow-up with a couple of vendors and will brief the task force on what he found.

Senator Fukunaga stated that the solution seems to be coming out of the electronic document management field. The technology involves scanning hard copy documents, optical character recognition and using screening tools, identifying the occurrence of personal information, and through an intelligent interface with the user, allow the user to either manually or automatically redact.

Investigative Working Groups – Reports:

Member Young reported that he recently met with the four county police departments and county prosecutors and asked them how the law regarding the possession of confidential information was working. They all reported that the law is very effective because criminals are now charged with a felony for possession of personal information. In the past, it was a misdemeanor or petty misdemeanor. The Notary Section of the Attorney General's Office is proposing a criminal bill for falsifying a notarized document. All notaries will be held to certain standards of reviewing documents they notarize for completeness. It would be considered a felony should the notary be in noncompliance. In addition, Member Young stated that the AG's office is also proposing that notaries verify identification as required. This bill is moving forward.

Member Young informed the task force that he has been in communication with Vice Chair Dang on whether or not the task force can introduce a bill relating to harassment through the internet. Member Young stated that it is very difficult to draft language that balances free speech against harassment directed at a particular person. Member Young stated that the problem is they would not be able to bring a criminal case in these types of situations. Chair Caulfield asked whether this issue is something the task force would like the AG's office or Member Young to explore.

Representative Meyer asked if there was a law regarding harassment over the phone. Member Young replied that there is a harassment statute that makes it a misdemeanor. It would be harassment to say things to others that may be threatening, or taken as threatening. Part of the problem, aside from drafting language that would be constitutional, would be finding the individuals. In Vice Chair Dang's case, they cannot identify the source of the emails, and the harassment statutes may not fit, as the emails are not threatening.

Member Takushi asked if there is a way the task force could start thinking about how to eliminate anonymous kinds of communication. Member Young stated that it is not a state issue. Most of the anonymous mailers are out-of-country.

Vice Chair Dang stated that California is looking at legislation that has to do with harassment through telephone, computers, and faxes. Vice Chair Dang will brief the task force on California's legislation.

Member Young asked if this issue is something the task force would like to address. Senator Fukunaga stated we could at least make people aware of some of the horror stories that are emerging. The ID theft and anti-phishing initiatives were started to help protect people. Member Young stated that this issue is another instance where there could be physical harm and can be a serious. Vice Chair Dang said in a situation like this, the victims are not necessarily just individuals. Businesses and politicians can also be victims of smear campaigns.

Member Levins distributed a draft document he prepared for businesses to use as best practices. He asked that the task force review the document and to provide him feedback so that the document can be finalized.

Chair Caulfield stated that he had nothing to report at this time regarding his working group.

Meeting Schedule: Chair Caulfield discussed the timeframe and remaining task force meetings to meet the task force legislation's requirement. Chair Caulfield also reiterated that the September 27th meeting has been cancelled and the October 25th meeting will be moved up a week or so. The Auditor's office will be polling the members on their availability.

State Auditor Higa stated that the members should be aware of the key meetings in November and December. The report needs to be submitted to the Legislature 20 days prior to start of session. Chair Caulfield also mentioned that the November 19th meeting is a critical one. Ms. Oshiro will follow up with members for quorum purposes.

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

With no further business, the Chair adjourned the meeting at 10:20 a.m.

Next Meeting: To be determined.

Reviewed and approved by:

Russell Wong
IT Coordinator

September 18, 2007

[ ] Approved as circulated.

ID Theft/090607