LATE

Good Afternoon Chair Fukunaga, Chair Tokuda distinguished members of the panel. Happy New Year.

My name is Debra Gagne. I am the Administrator for the Information and Communication Services Division within the Department of Accounting and General Services. I am here today to present information about the Information Privacy and Security Council.

In the next 10 minutes or so I hope to give you a better idea of

- What the IPSC is
- What the IPSC does
- What the IPSC has done
- What the IPSC is currently working on
- Recommendations on draft legislation

Safeguarding Personal information held by government agencies is absolutely necessary. We have been placed in a position of trust by the citizens of Hawai'I and it is our responsibility to assure that we deserve that trust. Social Security Numbers were the first area of personal information addressed with the Identity Task Force report published in December 2007. Social Security Numbers were the most ubiquitous piece of information we had and the most vulnerable to mis-use.

Some breach research bears this out. The Privacy Rights Clearinghouse at privacyrights.org reports on security breaches they become aware of. For the calendar year 2010, I did an assessment of breaches in the organization type of Government and found that 1,087,397 records had been compromised. Further more for the year, 78 breaches were reported on, and a statistically significant 74% or 58 of them involved Social Security Numbers. What I found particularly telling was that of

the breach incidents only 7 were the result on HACK events. The majority of reported breaches resulted from Unintended disclosure, Physical loss or Portable devices lost, stolen or discarded.

This type of information is what prompts the Information Privacy and Security Council to stress guidelines, best practices, awareness and education, coupled with personal accountability and responsibility.

What the IPSC is

The council was formed with the passage of SB2803, SC1, HD1, CD1 to protect the security of personal information collected and maintained by state and county government agencies.

The IPSC first met in September 2008 when it was instated by ACT 10 and was mandated to:

1. Develop guidelines to be considered by government agencies in deciding whether, how, and when a government agency shall inform affected individuals of the loss, disclosure, or security breach of personal information and that can contribute to identify theft

2. Review the individual annual reports submitted by government agencies, and submit a summary report to the Legislature.

3. Identify best practices to assist government agencies in improving security and privacy programs relating to personal information.

What the IPSC does

The Council is a sunshine law committee meeting and meets on a monthly basis when there is sufficient quorum. The council members represent the following areas as required by Act 10:

Council Membership

Dept. of Accounting and General Services	**Coppa, Bruce.** - State Comptroller **(Chair)**
	Au Paul K.W. - EPS Compliance Manager
City and County of Honolulu	**Kam, Geoffrey M.** -Deputy Corporation Counsel (Designee)
	Tsuchiya, Burt -Director of Data Systems
County of Hawai‘i	**Kiley, James** -Data Systems Manager (Designee)
	(Vacant)
County of Kaua‘i	**Norman, Nyree** - Information Technology Specialist (Designee)
	Verkerke, **Jacob** - Information Systems Manager
County of Maui	**Underwood, Susan** -Information Management Section Head (Designee)
	Decasa, Meliton Jr., - Data Processing Specialist
Dept. of Education	**Stone, Allan** -Director, Information Systems Svcs Br (Designee)
Dept. of Health	**Tseu , Andrew W.L.** - HIPAA Compliance

	Officer (Alternate Chair)
Dept. of Human Resources Development	**Merez, Gino** - HIPAA Specialist (Designee)
	Keane, **David** - Data Processing Systems Manager
	Miyasato, Kyle -Personnel Management Specialist (Designee)
Dept. of Human Services	**Oliva**, **Henry -** Deputy Director
	Yong, Lim -DHS HIPAA Coordinator (Designee)
House (Senate Appointee)	**Mau-Shimizu**, **Patricia** - House Chief Clerk
	(Vacant) (Designee)
Judiciary	**Stathis, Christopher** - Director, Support Services
	Gochros , Susan Pang - Inter-Government & Community Relations (Designee)
University of Hawai‘i	**Lassner, David -** UH Board of Regents
	Ito , Jodi - Information Security Officer (Designee

In the absence of any staff resources aligned with the Council, Todd Crosby, Assistant Administrator, ICSD has taken on the role of Acting Executive Director. His contribution has included much of the research, Cyber Security office in ICSD involvement, as well as document creation.

What the IPSC has done

The IPSC created a website IPSC.hawaii.gov to provide open and transparent information to the public regarding their activities.

In July of 2009 the IPSC provided Guidelines on informing individuals of loss of PII or breach, and then further amended the breach policy in December 2010.

The first Council summary of agency reports to the Legislature was delivered in December 2009, the next in April 2010. The report for FY2010 is in progress.

The council identified, published and assured that best practices were posted in each agency's website for the following topics:

- Breach Best Practices
- Security of Laptops, Removable Data Storage, Devices, and Communication Devices
- A quick reference to many industry best practices, tools, and resources for information security as identified by the Information Privacy and Security Council.

The Council spearheaded the effort to insure that the Privacy policy on State websites was consistent

Notified agencies to develop plans to eliminate the unnecessary use of SSN in September 2008 and collected the resulting reports.

What the IPSC is currently working on

Gathering information from the various agencies for the Fiscal year 2010 report to the Legislature.

Breach Notification templates for use by agencies to include such elements as letters, Legislative report formats etc.

Developing guidelines for the secure use of digital document equipment (printers, copiers, scanners)

Legislative Recommendations

In reviewing the DRAFT bill provided, the IPCS has some specific comments relative to awareness, training, staffing and technology.

1. If the scope of the bill were to be expanded, the Council would suggest a confidential study on the state of cyber security in Hawai‘i government and recommendations to address the issues (e.g., governance, authority, etc.) brought up in the study. In order to be effective, we need to look at the whole picture and not just slices of the pie. Otherwise, we could simply focus on training, as understood in the draft legislation.

2. As for privacy and cyber security training, we would expect ICSD to be the technical experts in Cyber-Security topics by developing awareness of what should be done, risks involved, and understanding of consequences for non-compliance. We would not expect each agency to develop their own training. We envision a base level curriculum made up of computer based training that agencies can use "as is", and either tailor to their specific circumstances or supplement with agency specific hands-

on training. Once the base modules are developed they could be turned over to DHRD to manage, coordinate enrollment, and track attendance to report back to the IPSC regarding compliance. At least annually, ICSD would review the curriculum and create updates as needed.

3. Relieve individual departments from having to be experts in security training, tools, regulations, basic laws, and policies that apply to agencies statewide. Let them trust that ICSD will do that and let them know if they are out of synch. Agencies can then concentrate on privacy and security issues specific to their agency. (e.g. Hippa etc.)

4. A study should be commissioned to examine where State systems or processes utilize SSN numbers when not required by federal or other mandate. Determine if an employee number or other identifying number could be used, and determine the costs and staffing needs to update these systems.

5. The IPSC recommends that a statewide committee be established that follows the structure and function recommendations laid out in the National Institute of Standards (NIST) Special Publication 800-39 draft "Integrated Enterprise-Wide Risk Management Organization, Mission, and Information System View", which can be downloaded from http://csrc.nist.gov/publications/drafts/800-39/draft-SP800-39-FPD.pdf

STAFFING REQUIREMENTS

To properly carry out the spirit of this bill, it is felt that the staffing that was not included in the original Act 10 be properly addressed.

The bare minimum staff and what their duties could consist of include:

- Statewide Security Scanning Coordinator (1)
  Provide real Time ongoing scanning as the ICSD does today, but extended and expanded statewide and include features ICSD currently does not have such as SSN filters, TripWire type tools for change detection, Websense for traffic monitoring, etc.

- Statewide Network Security Coordinator (1)
  Provide analysis of Firewall placement and rule sets. Establishes general enforceable guidelines for all firewall definitions statewide. Authority to scan across and through firewalls to check for exposure to inadvertent penetration. Responsible for coordination of an annual external security audit (could be federal or private), and report to IPSC of findings and the required management response for corrective action similar to the current ICSD SAS/70 audits but at the network level. If the State used managed services in selected areas, this position would be the managed services watchdog.

- Statewide Application Scanning Service Specialist (1)
  Provide departments and agencies with ongoing active scanning, and reports on their applications that may expose any programming faults that have the potential to provide hackers with access to confidential information. Findings would be tracked and reported to the IPSC, and provide the required management response for corrective action. Provide annual application audit for selected public facing applications.

- Security Incident Specialist (1)
  Breaches will be coordinated through ICSD for awareness, understanding, and documentation. The breach expert will facilitate the inclusion of appropriate legal, law enforcement, public information officer, and compliance entities. This would include the use of standardized reporting templates and communication models.

- Training Coordinator(1)
- A training coordinator directly addresses the draft legislation. Self directed learning may create familiarity with policies, best practices and guidelines but may not always surface the risks that exist the way individual education can. It needs to be ensured that DHRD is on board, able, and willing to assist as this would be a statewide training effort that requires accountability.

- Clerical/Administrative Support (1)
  Provide IPSC support for the necessary added reporting, scheduling, and follow-up required to facilitate the knowledge the IPSC needs for training, data scanning, network security, application scanning compliance, incident coordination, and reporting.

ESTIMATED STAFF COSTS: 5 * 70,000 = $350,000 + 40% = $490,000 annual operating. It is suggested that the staff be housed as part of the ICSD Cyber Security Team and provides reports to IPSC through

Security Tools, Maintenance & Licenses

The State does not own sufficient modern automated tools that can automate the detection of security or breach issues. Doing so by hand, given the breadth of systems that the State maintains, is not technically feasible. Below is a recommendation of the minimum amount of tools required to provide a basic level of protection and detection. It is highly recommended to ensure that the State receives the maximum vendor discounts that these items be procured on a statewide basis and not agency by agency, and that State procurement modifications are made to allow us to take advantage of established Federal DOD programs and discount levels.

- Statewide change management software to detect unauthorized changes in cyber security systems, systems containing PII, application code, and configuration files.
- Expansion of existing web application scanning software (ATG and ICSD have some basic software already).
- Expansion of active security monitoring software.
- Mandatory managed anti-virus for all State owned servers, desktops, and laptops.
- Mandatory disk encryption for laptops that contain PII.
- Mandatory anti-spam / anti-virus scanning for all e-mailboxes.
- Estimated cost for the above: $875,000 initially for acquisition, with $170,000 annual operating costs. Note that existing staffing levels could not feasibly implement and manage these new tools.

- **Thank you Senators for the opportunity to address this briefing. I hope that I sufficiently addressed**
  - What the IPSC is
  - What the IPSC does
  - What the IPSC has done
  - What the IPSC is currently working on, AND
  - Recommendations

I would like to end my remarks with several pertinent quotes:

People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. — Bruce Schneier, Secrets and Lies

Security is always excessive until it's not enough. — Robbie Sinclair, Head of Security, Country Energy, NSW Australia

The Information Super-highway is the only highway you don't need a license, an education or insurance to use….Debra Gagne

And Lastly one of the areas in the ICSD is the CyberSecurity Office. As part of our involvement in the nationwide MS-ISAC (Multi State – Information Sharing and Analysis Center) --- this is where we receive information about security vulnerabilities we send out to IT representatives statewide --- I have brought with me some of the Cyber Security awareness materials they provide in the form of calendars and bookmarks. Please help yourselves and share them with your friends.