ACT 10

S.B. NO. 2803

A Bill for an Act Relating to Personal Information.

Be It Enacted by the Legislature of the State of Hawaii:

PART I

SECTION 1. The purpose of this Act is to implement the recommendations of the December 2007 report of the Hawaii identity theft task force to protect the security of personal information collected and maintained by state and county government agencies.

PART II

SECTION 2. Chapter 487J, Hawaii Revised Statutes, is amended by adding a new section to be appropriately designated and to read as follows:

"**§487J-A Policy and oversight responsibility.** (a) By September 1, 2009, each government agency shall designate an agency employee to have policy and oversight responsibilities for the protection of personal information.

(b) The designated agency employee shall:

(1) Ensure and coordinate agency compliance with this chapter, chapter 487N, and chapter 487R;

(2) Assist individuals who have identity theft and other privacy-related concerns;

(3) Provide education and information to agency staff on privacy and security issues;

(4) Coordinate with state, county, and federal law enforcement agencies on identity theft investigations; and

(5) Recommend policies and practices to protect individual privacy rights relating to the individual's personal information."

SECTION 3. Section 487J-1, Hawaii Revised Statutes, is amended by adding a new definition to be appropriately inserted and to read as follows:

""Personal information" has the same meaning as in section 487N-1."

SECTION 4. Chapter 487N, Hawaii Revised Statutes, is amended by adding three new sections to be appropriately designated and to read as follows:

"**§487N-A Information privacy and security council; established; duties; reports.** (a) There is established an information privacy and security council within the department of accounting and general services for administrative purposes only. Members of the council shall be appointed no later than September 1, 2008, by the governor without regard to section 26-34 and shall be composed of the following representatives:

(1) Executive agencies that maintain extensive personal information in the conduct of their duties, including the department of education, the department of health, the department of human resources development, the department of human services, and the University of Hawaii, to be selected by the governor;
(2) The legislature, to be selected by the president of the senate and the speaker of the house of representatives;
(3) The judiciary, to be selected by the administrator of the courts; and
(4) The four counties, to be selected by the mayor of each county; provided that the mayor of each county shall determine the extent to which the county may or may not participate.

The comptroller shall serve as chair of the council.

(b) By January 1, 2009, the council shall submit to the legislature a report of the council's assessment and recommendations on initiatives to mitigate the negative impacts of identity theft incidents on individuals. The report shall emphasize assessing the merits of identity theft passport and identity theft registry initiatives that have been implemented in other states.

(c) No later than June 30, 2009, the council shall 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 that can contribute to identify theft. The guidelines shall provide a standardized, risk-based notification process in the instance of a security breach.

(d) The council shall review the individual annual reports submitted by government agencies, pursuant to section 487N-C and submit a summary report to the legislature no later than twenty days prior to the convening of the regular session of 2010 and each year thereafter. The summary report shall include the council's findings, significant trends, and recommendations to protect personal information used by government agencies.

The initial report to the legislature also shall include proposed legislation to amend section 487N-2 or any other law that the council deems necessary to conform to the guidelines established under subsection (c).

(e) The comptroller may establish support positions for the information and communication services division, including but not be limited to, legal support, information technology, human resources and personnel, records management, and administrative support.

§487N-B Personal information security; best practices; websites. (a) The council shall identify best practices to assist government agencies in improving security and privacy programs relating to personal information. No later than March 31, 2009, the council shall identify best practices relating to:

(1) Automated tools;
(2) Training;
(3) Processes; and
(4) Applicable standards.

(b) No later than July 31, 2009, the best practices identified by the council shall be posted on each government agency's website in a manner that is readily accessible by employees of the government agency.

§487N-C Personal information system; government agencies; annual report. (a) Effective January 1, 2009, any government agency that maintains one or more personal information systems shall submit to the council an annual report on the existence and character of each personal information system added or eliminated since the agency's previous annual report. The annual report shall be submitted no later than September 30 of each year.

(b) The annual report shall include:
(1) The name or descriptive title of the personal information system and its location;
(2) The nature and purpose of the personal information system and the statutory or administrative authority for its establishment;
(3) The categories of individuals on whom personal information is maintained, including:
  (A) The approximate number of all individuals on whom personal information is maintained; and
  (B) The categories of personal information generally maintained in the system, including identification of records that are:
    (i) Stored in computer accessible records; or
    (ii) Maintained manually;
(4) All confidentiality requirements relating to:
  (A) Personal information systems or parts thereof that are confidential pursuant to statute, rule, or contractual obligation; and
  (B) Personal information systems maintained on an unrestricted basis;
(5) Detailed justification of the need for statutory or regulatory authority to maintain any personal information system or part thereof on a confidential basis for all personal information systems or parts thereof that are required by law or rule;
(6) The categories of sources of personal information;
(7) The agency's policies and practices regarding personal information storage, duration of retention of information, and elimination of information from the system;
(8) The uses made by the agency of personal information contained in any personal information system;
(9) The identity of agency personnel, by job classification, and other agencies, persons, or categories to whom disclosures of personal information are made or to whom access to the personal information system may be granted, including the purposes of access and any restrictions on disclosure, access, and redisclosure;
(10) A list identifying all forms used by the agency in the collection of personal information; and
(11) The name, title, business address, and telephone number of the individual immediately responsible for complying with this section.

(c) For purposes of this section:

"Personal information system" means any manual or automated recordkeeping process that contains personal information and the name, personal number, or other identifying particulars of a data subject.

(d) Notwithstanding any other law to the contrary, this report shall be confidential and not disclosed publicly in any form or forum."

SECTION 5. Section 487N-1, Hawaii Revised Statutes, is amended by adding a new definition to be appropriately inserted and to read as follows:

""Council" means the information privacy and security council established under section 487N-A."

PART III

SECTION 6. Act 137, Session Laws of Hawaii 2006, as amended by Act 183, Session Laws of Hawaii 2007, section 11, is amended by amending section 3 to read as follows:

"SECTION 3. This Act shall take effect on July 1, [~~2008.~~] 2009."

PART IV

SECTION 7. Practices and procedures relating to security of laptops, removable data storage devices, and communication devices. By December 31, 2008, the information privacy and security council established under section 487N-A, Hawaii Revised Statutes, in consultation with the information and communication services division of the department of accounting and general services, and the information technology divisions of the respective counties, shall develop recommended practices and procedures to provide guidance to information technology managers in all government agencies relating to the security of laptops, removable data storage devices, and communication devices used to remotely access applications installed on state or county networks. The council shall include recommendations on best practices and standards for protecting personal information that may be used with, stored on, or transmitted by the foregoing devices.

PART V

SECTION 8. Third party personal information use contractual provisions. (a) Effective September 1, 2008, any government agency that:

(1) Contracts with third parties to provide support services on behalf of the agency that requires access to personal information; or

(2) Is requested to provide access to social security numbers and other personal information by a credit bureau or similar financial reporting organization,

shall include, in all new or renewed contracts, provisions to protect the use and disclosure of personal information administered by the agency. In developing these provisions, the agency shall take into consideration similar restrictive provisions, included in the Fair Credit Reporting Act (15 U.S.C. section 1681f and 15 U.S.C. section 1681 et seq.) and shall attempt to make the agency's provisions similar to those in the Fair Credit Reporting Act. Consumer Reporting Agencies, as defined by 15 U.S.C. section 1681a(f) that operate under and are in compliance with 15 U.S.C. section 1681 et seq, shall be deemed to be in compliance with Hawaii law and shall be entitled to a rebuttable presumption of compliance.

(b) Provisions relating to personal information protection in contractual agreements with third parties shall require consistent with subsection (a)(2):

(1) Implementation of technological safeguards acceptable to the government agency to reduce exposure to unauthorized access to personal information;
(2) Mandatory training on security awareness topics relating to personal information protection for employees of the third party;
(3) Confidentiality agreements to be signed by third party employees acknowledging that:
    (A) The personal information collected, used, or maintained by the government agency is confidential;
    (B) Access to the personal information is restricted to the minimum necessary; and
    (C) Use of the personal information is restricted to uses consistent with the services subject to the contractual agreement;
(4) Clarification that no personal information shall be retained or used for a purpose other than that for which it was originally collected and all copies of personal information records provided by the government agency to the third party shall be destroyed by the third party at the conclusion of the contract;
(5) Prompt and complete disclosure of security breaches; and
(6) A complete log of disclosures made of the government agency personal information.

As used in this section, "technological safeguards" means the technology and the policy and procedures for use of the technology to protect and control access to personal information.

PART VI

SECTION 9. (a) Protection of personal information by government agencies. No later than September 1, 2008, all government agencies that collect, maintain, or disseminate documents containing personal information that are subject to disclosure pursuant to section 92F-12, Hawaii Revised Statutes, shall develop and implement a plan to protect and redact personal information, specifically social security numbers, contained in any existing hardcopy documents prior to making the documents available for public inspection. Consumer reporting agencies, as defined by 15 U.S.C. section 1681a(f), which operate under 15 U.S.C. section 1681 et seq., shall continue to have access to personal information, including the nine digit social security numbers as the legislature finds that such access is necessary for criminal background checks, credit reporting for financial transactions and other similar purposes. Agency plans shall be consistent with these purposes.

(b) Written report. Any government agency that fails to develop and implement a plan to protect and redact personal information by September 1, 2008, shall submit to the legislature by September 30, 2008, a written report that details information relating to any documents that contain social security numbers that were disclosed pursuant to section 92F-12, Hawaii Revised Statutes. The written report shall identify the document disclosed, including the date, nature, and purpose of each disclosure and the name and address of the person to whom the disclosure was made. The written report shall not include any disclosure made to the individual to whom the personal information refers.

SECTION 10. Budgets. The proposed budget for the development and implementation of the plan to protect and redact personal information in existing, hardcopy records shall be prepared by December 31, 2008, by each government agency, for submittal as part of the respective executive, judiciary, and legislative budgets.

PART VII

SECTION 11. Plan to reduce collection and use of social security numbers. No later than December 1, 2008, all government agencies that collect, maintain, or disseminate documents containing personal information that are subject to disclosure pursuant to section 92F-12, Hawaii Revised Statutes, shall develop a written plan to eliminate the unnecessary collection and use of social security numbers. In developing such plans, the agencies shall consider that consumer reporting agencies, as defined by 15 U.S.C. section 1681a(f), which operate under 15 U.S.C. section 1681 et seq., shall continue to have access to personal information, including the nine digit social security numbers as the legislature finds that such access is necessary for criminal background checks, credit reporting for financial transactions and other similar purposes. Agency plans shall be consistent with these purposes.

Each plan shall include provisions to require:

(1) The collection and use of social security numbers only when required by federal or state law, or when the social security number is the only identifier currently available;

(2) When required by federal or state law to collect social security numbers, or when the social security number is the only identifier currently available, the agency to proceed as reasonably necessary for the proper administration of lawful agency business; and

(3) The development of an alternative unique identifier number to replace current discretionary use of social security numbers.

Agencies shall submit their plan for review and comment to the information privacy and security council established by section 487N-A, Hawaii Revised Statutes, no later than December 1, 2008.

SECTION 12. Funding request. Each government agency shall submit to the 2009 regular session of the legislature a funding request for fiscal year 2009-2010 for an amount necessary to implement the agency's plan to eliminate the unnecessary collection or use of social security numbers.

PART VIII

SECTION 13. (a) Guidance on recommended human resources practices to protect personal information. No later than January 1, 2010, the lead state and county government agencies that have primary responsibility for human resource functions shall develop and distribute to the appropriate government agencies written guidelines detailing recommended practices to minimize unauthorized access to personal information and personal information systems relating to personnel recruitment, background checks, testing, employee retirement and health benefits, time reporting and payroll issues. The recommended practices shall address, at a minimum:

(1) Physical safeguards for paper and electronic records stored onsite and offsite, as well as for removable storage media that includes laptop computers, USB storage devices, compact discs, and tapes;

(2) Administrative safeguards to control and monitor access to human resources personal information systems; and

(3) Technological safeguards to ensure the confidentiality and integrity of information transmitted over computer networks, laptop computers, and removable storage devices.

(b) Definitions. For the purpose of this part:

"Administrative safeguards" means administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of

security measures to protect personal information and to manage the conduct of the workforce in relation to the protection of personal information.

"Physical safeguards" means physical measures, policies, and procedures to protect personal information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

PART IX

SECTION 14. (a) Security breach notification policy. No later than September 1, 2009, all government agencies shall develop a written agency policy relating to notification of any security breach of personal information. The policy shall ensure appropriate safeguards to protect personal information and shall apply to electronic system and paper document records that contain personal information.

The security breach notification policy for government agencies shall consider guidelines established by the information privacy and security council under section 487N-A Hawaii Revised Statutes, and shall include provisions to determine:

(1) Whether security breach notification is required;
(2) The timeliness of the notification;
(3) The source of the notification;
(4) The contents of the notification;
(5) The manner in which notification shall be provided; and
(6) Recipients of notification.

(b) Security breach notification policy review and amendment. No later than September 1, 2009, all government agencies shall submit their security breach notification policy to the attorney general, appropriate corporation counsel, or county attorney for review and comment. A government agency's security breach notification policy shall be promptly amended to incorporate revisions recommended by the attorney general, corporation counsel, or county attorney after review of the security breach notification policy.

Beginning December 31, 2010, government agencies shall review their security breach notification policies by December 31 annually and make amendments as necessary. Information relating to a government agency's security breach notification policy, including any amendments, shall be disseminated to the appropriate employees in each government agency.

PART X

SECTION 15. Definitions. For purposes of this Act:

"Government agency" has the same meaning as in section 487N-1, Hawaii Revised Statutes.

"Personal information" has the same meaning as in section 487N-1, Hawaii Revised Statutes.

"Personal information system" means any manual or automated recordkeeping process that contains personal information and the name, personal number, or other identifying particulars of a data subject.

"Records" has the same meaning as in section 487N-1, Hawaii Revised Statutes.

"Security breach" has the same meaning as in section 487N-1, Hawaii Revised Statutes.

SECTION 16. In codifying the new sections added by sections 2 and 4 of this Act, the revisor of statutes shall substitute appropriate section numbers for the letters used in designating the new sections in this Act.

PART XI

SECTION 17. (a) There is established no later than July 1, 2008, within the office of the auditor, the identity theft task force working group, to:

(1) Provide continuity from the work of the identity theft task force, established pursuant to Act 65, Session Laws of Hawaii 2005, as amended by Act 140, Session Laws of Hawaii 2006; and

(2) Assist in the transition and development of recommendations and best practices related to personal information.

(b) The working group shall include five members of the identity theft task force, the auditor, and the consultant retained by the auditor for the work of the identity theft task force.

(3)[1] The identity theft task force working group shall cease to exist on June 30, 2009.

SECTION 18. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.[2]

SECTION 19. This Act shall take effect on July 1, 2008; provided that section 6 shall take effect on June 30, 2008.

(Vetoed by Governor and veto overridden by Legislature on July 8, 2008.)

Notes

1. So in original.
2. Edited pursuant to HRS §23G-16.5.