Select Committee to Protect Personal Information

Monday, February 4, 2008
1:00 PM – 3:00 PM
Morris Hall

Marco Rubio
Speaker

William L. Proctor
Chairman

Committee Meeting Notice

HOUSE OF REPRESENTATIVES

Speaker Marco Rubio

Select Committee to Protect Personal Information

Start Date and Time:	Monday, February 04, 2008 01:00 pm
End Date and Time:	Monday, February 04, 2008 03:00 pm
Location:	Morris Hall (17 HOB)
Duration:	2.00 hrs

Workshop on the following:

Recommendations submitted to the Select Committee

NOTICE FINALIZED on 01/28/2008 16:03 by TUCK.SHIRLEY

TABLE OF CONTENTS

RECOMMENDATIONS SUBMITTED BY REP. LONG:

Proposals:

The first proposal deals with certifying vendors that work with state contracts to ensure that companies and their employees who may be handling sensitive information have been trained on various privacy and data security standards provided by the International Association of Privacy Professionals.

The second proposal would create the position of Chief Privacy Officer and a team of auditors under the Department of Management Services to create a report card assessment for the Governor and public on how well our executive, legislative, and judicial branches are performing as it related to the secure collection and storage of personal information.[1]

[1] Submitted via letter to Chair Proctor, January 23, 2008 (copy on file with the Select Committee to Protect Personal Information).

Florida House of Representatives

Representative Janet C. Long

District 51

District Office:
5511 Park Street North, Suite 101
St. Petersburg, FL 33709
727/545-6421
727/545-6423 (Fax)

Tallahassee Office:
1402 The Capitol
402 South Monroe Street
Tallahassee, FL 32399
850/488-6197

January 23, 2008

The Honorable William Proctor, Chairman
Select Committee to Protect Personal Information
317 HOB, 402 S Monroe Street N
Tallahassee, FL 32399

Dear Chairman Proctor,

Thank you so much for your leadership of the Select Committee to Protect Personal Information. I so appreciate the hard work you and the committee staff have undertaken to educate us on the issues surrounding identity theft. I am particularly grateful for your invitation to share input as we develop a committee bill that we can all be proud of and that will serve to protect the citizens of Florida.

I am writing to you today to share two ideas that I discussed with Keith Carr, the President of ID Theft Solutions, a Tallahassee-based firm.

The first proposal deals with certifying vendors that work with state contracts to ensure that companies and their employees who may be handling sensitive information have been trained on various privacy and data security standards provided by the International Association of Privacy Professionals.

The second proposal would create the position of Chief Privacy Officer and a team of auditors under the Department of Management Services to create a report card assessment for the Governor and public on how well our executive, legislative, and judicial branches are performing as it relates to the secure collection and storage of personal information.

Thank you for your consideration of the above proposals and I look forward to continuing to work with you on these important issues. Please let me know if I can be of any assistance.

With warm personal regards,

Janet C. Long

2

RECOMMENDATIONS SUBMITTED BY REP. ADAMS:

I would like to see us focus on state agencies.

I would like to focus on how personal information is gathered by state agencies, the need for such information (is it because the form has Social Security numbers listed, etc.), how the information is retained, how is it released (for what purpose, etc.), and how it is disposed of once it is no longer needed (shredded, burned, etc.)?[1]

[1] Submitted via email on January 29, 2008 (on file with the Select Committee to Protect Personal Information).

119.021 Custodial requirements; maintenance, preservation, and retention of public records.—

(1) Public records shall be maintained and preserved as follows:

(a) All public records should be kept in the buildings in which they are ordinarily used.

(b) Insofar as practicable, a custodian of public records of vital, permanent, or archival records shall keep them in fireproof and waterproof safes, vaults, or rooms fitted with noncombustible materials and in such arrangement as to be easily accessible for convenient use.

(c)1. Record books should be copied or repaired, renovated, or rebound if worn, mutilated, damaged, or difficult to read.

2. Whenever any state, county, or municipal records are in need of repair, restoration, or rebinding, the head of the concerned state agency, department, board, or commission; the board of county commissioners of such county; or the governing body of such municipality may authorize that such records be removed from the building or office in which such records are ordinarily kept for the length of time required to repair, restore, or rebind them.

3. Any public official who causes a record book to be copied shall attest and certify under oath that the copy is an accurate copy of the original book. The copy shall then have the force and effect of the original.

(2)(a) The Division of Library and Information Services of the Department of State shall adopt rules to establish retention schedules and a disposal process for public records.

(b) Each agency shall comply with the rules establishing retention schedules and disposal processes for public records which are adopted by the records and information management program of the division.

(c) Each public official shall systematically dispose of records no longer needed, subject to the consent of the records and information management program of the division in accordance with s. 257.36.

(d) The division may ascertain the condition of public records and shall give advice and assistance to public officials to solve problems related to the preservation, creation, filing, and public accessibility of public records in their custody. Public officials shall assist the division by preparing an inclusive inventory of categories of public records in their custody. The division shall establish a time period for the retention or disposal of each series of records. Upon the completion of the inventory and schedule, the division shall, subject to the availability of necessary space, staff, and other facilities for such purposes, make space available in its records center for the filing of semicurrent records so scheduled and in its archives for noncurrent records of permanent value, and shall render such other assistance as needed, including the microfilming of records so scheduled.

(3) Agency orders that comprise final agency action and that must be indexed or listed pursuant to s. 120.53 have continuing legal significance; therefore, notwithstanding any other provision of this chapter or any provision of chapter 257, each agency shall permanently maintain records of such orders pursuant to the applicable rules of the Department of State.

(4)(a) Whoever has custody of any public records shall deliver, at the expiration of his or her term of office, to his or her successor or, if there be none, to the records and information management program of the Division of Library and Information Services of the Department of State, all public records kept or received by him or her in the transaction of official business.

(b) Whoever is entitled to custody of public records shall demand them from any person having illegal possession of them, who must forthwith deliver the same to him or her. Any person unlawfully possessing public records must within 10 days deliver such records to the lawful custodian of public records unless just cause exists for failing to deliver such records.

History.—s. 2, ch. 67-125; s. 3, ch. 83-286; s. 753, ch. 95-147; s. 5, ch. 2004-335.

119.071 General exemptions from inspection or copying of public records.—

(5) OTHER PERSONAL INFORMATION.—

1.a. The Legislature acknowledges that the social security number was never intended to be used for business purposes but was intended to be used solely for the administration of the federal Social Security System. The Legislature is further aware that over time this unique numeric identifier has been used extensively for identity verification purposes and other legitimate consensual purposes.

b. The Legislature recognizes that the social security number can be used as a tool to perpetuate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual.

c. **The Legislature intends to monitor the use of social security numbers held by agencies in order to maintain a balanced public policy.**

2.a. **An agency may not collect an individual's social security number unless the agency has stated in writing the purpose for its collection and unless it is:**

(I) Specifically authorized by law to do so; or

(II) Imperative for the performance of that agency's duties and responsibilities as prescribed by law.

b. Social security numbers collected by an agency may not be used by that agency for any purpose other than the purpose provided in the written statement.

3. An agency collecting an individual's social security number shall provide that individual with a copy of the written statement required in subparagraph 2.

4.a. **Each agency shall review whether its collection of social security numbers is in compliance with subparagraph 2. If the agency determines that collection of a social security number is not in compliance** with subparagraph 2., **the agency shall immediately discontinue the collection** of social security numbers for that purpose.

b. **Each agency shall certify to the President of the Senate and the Speaker of the House of Representatives its compliance with this subparagraph no later than January 31, 2008.**

257.36 Records and information management.—

(1) There is created within the Division of Library and Information Services of the Department of State a records and information management program. It is the duty and responsibility of the division to:

(a) Establish and administer a records management program directed to the application of efficient and economical management methods relating to the creation, utilization, maintenance, retention, preservation, and disposal of records.

(b) Establish and operate a records center or centers primarily for the storage, processing, servicing, and security of public records that must be retained for varying periods of time but need not be retained in an agency's office equipment or space.

(c) Analyze, develop, establish, and coordinate standards, procedures, and techniques of recordmaking and recordkeeping.

(d) Ensure the maintenance and security of records which are deemed appropriate for preservation.

(e) Establish safeguards against unauthorized or unlawful removal or loss of records.

(f) Initiate appropriate action to recover records removed unlawfully or without authorization.

(g) Institute and maintain a training and information program in:

1. All phases of records and information management to bring approved and current practices, methods, procedures, and devices for the efficient and economical management of records to the attention of all agencies.

2. The requirements relating to access to public records under chapter 119.

(h) Provide a centralized program of microfilming for the benefit of all agencies.

(i) Make continuous surveys of recordkeeping operations.

(j) Recommend improvements in current records management practices, including the use of space, equipment, supplies, and personnel in creating, maintaining, and servicing records.

(k) Establish and maintain a program in cooperation with each agency for the selection and preservation of records considered essential to the operation of government and to the protection of the rights and privileges of citizens.

(l) Make, or have made, preservation duplicates, or designate existing copies as preservation duplicates, to be preserved in the place and manner of safekeeping as prescribed by the division.

(2)(a) All records transferred to the division may be held by it in a records center or centers, to be designated by it, for such time as in its judgment retention therein is deemed necessary. At such time as it is established by the division, such records as are determined by it as having historical or other value warranting continued preservation shall be transferred to the Florida State Archives.

(c) When a record held in a records center is eligible for destruction, the division shall notify, in writing, by certified mail, the agency which transferred the record. The agency shall have 90 days from receipt of that notice to respond requesting continued retention or authorizing destruction or disposal of the record. If the agency does not respond within that time, title to the record shall pass to the division.

(5) For the purposes of this section, the term "agency" shall mean any state, county, district, or municipal officer, department, division, bureau, board, commission, or other separate unit of government created or established by law. It is the duty of each agency to:

(a) Cooperate with the division in complying with the provisions of this chapter and designate a records management liaison officer.

(b) Establish and maintain an active and continuing program for the economical and efficient management of records.

(6) A public record may be destroyed or otherwise disposed of only in accordance with retention schedules established by the division. The division shall adopt reasonable rules not inconsistent with this chapter which shall be binding on all agencies relating to the destruction and disposition of records. Such rules shall provide, but not be limited to:

(a) Procedures for complying and submitting to the division records-retention schedules.

(b) Procedures for the physical destruction or other disposal of records.

(c) Standards for the reproduction of records for security or with a view to the disposal of the original record.

History.—s. 5, ch. 67-50; ss. 10, 35, ch. 69-106; s. 4, ch. 81-173; s. 24, ch. 83-339; s. 46, ch. 86-163; s. 8, ch. 95-296; s. 34, ch. 2000-258; s. 15, ch. 2004-335.

Note.—Former s. 267.051.

3

RECOMMENDATIONS SUBMITTED BY REP. BRISE:

The following are my recommendations to the Select Committee to Protect Personal Information for consideration by the Florida House of Representatives:

1. The State of Florida or push for the business sector to establish protocols for businesses to standardize the method in which customer data found on credit cards and debit cards are managed and discarded based on best practices.

2. The Florida House of Representatives should propose a statute banning the use of card readers which do not truncate credit card and debit card numbers.[1]

[1] Submitted via email on January 31, 2008 (on file with the Select Committee to Protect Personal Information).

4

RECOMMENDATIONS SUBMITTED BY KEVIN FREIN:

STATUTORY AMENDMENTS

- Section 831.28(2)(a), F.S., counterfeiting a payment instrument – amend this statute to make the manufacturing/counterfeiting of a payment instrument a second degree felony with an offense severity ranking of seven.

- Section 817.568(1)(d), F.S., criminal use of personal identification information – amend the definition of "individual" to include a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity.[1]

- Section 901.1505(2), F.S., federal law enforcement officers – amend this statute to give federal law enforcement officers peace officer status/arrest powers for crimes enumerated under chapters 817 and 831, F.S.

STATUTORY ENACTMENTS

- Create a statute setting standards for businesses for the safeguard and disposal of personal identification information. At a minimum this statute should include a requirement that businesses shred or destroy documents that contain personal identification information as defined under chapter 817, F.S.[2]

- Create a statute that provides an identity theft enhancement. Specifically, a statute that provides if during the commission of a felony and individual uses the personal identification of another person the felony is reclassified one degree.

FLORIDA HIGHWAY PATROL / DEPARTMENT OF HIGHWAY SAFETY & MOTOR VEHICLES

- Provide funding for the purchase of facial recognition software for use by the FHP/DHSMV in determining victims of identity theft.

---

[1] Currently, s. 817.568(1)(d), F.S., defines "individual" to mean "a single human being and does not mean a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity."

[2] Section 817.568(1)(f), F.S., defines "personal identification information" to mean "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:
1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code;
4. Medical records;
5. Telecommunication identifying information or access device; or
6. Other number or information that can be used to access a person's financial resources."

- Provide funding for the placement of Troopers at DMV Offices.

LAW ENFORCEMENT TRAINING

- The Florida Department of Law Enforcement (FDLE) is tasked with setting the mandatory training requirements for an individual to become a certified law enforcement officer. This training should be amended to include a block of instruction on the investigation of identity theft crimes.

- The FDLE Computer Division provides training on the investigation of computer related crimes. This training is primarily focused on law enforcement. An outreach program specifically targeting prosecutors throughout the state would provide more prosecutors with the requisite knowledge to handle these types of cases.

STATE ATTORNEY'S OFFICE

- Enact a legislative mandate that requires each SAO to designate two Assistant State Attorney's as "identity theft" prosecutors. This would ensure each judicial circuit has subject matter experts that can assist both law enforcement and victims of identity theft.[3]

[3] Submitted via letter to Chair Proctor, December 21, 2007 (copy on file with the Select Committee to Protect Personal Information).

STATE ATTORNEY
Fourth Judicial Circuit of Florida
Special Prosecution Division
10 West Adams Street, Suite 200
Jacksonville, Florida 32202-3618
Tel: (904) 351-0900
Fax: (904) 351-0929

HARRY L. SHORSTEIN
STATE ATTORNEY

A. JAY PLOTKIN
CHIEF ASSISTANT

December 21, 2007

The Honorable Representative Bill Proctor, District 20
Florida House of Representatives
900 SR 16, Suite 2
St. Augustine, Florida 32804

RE: IDENTITY THEFT RECOMMENDATIONS

Dear Representative Proctor:

Please accept this letter as a follow up to my testimony before the Select Committee to Protect Personal Information on December 11th, 2007. Pursuant to your request listed below are my recommendations to your committee regarding improving the State's ability to effectively combat identity theft:

Statutory Amendments

1. Counterfeiting a Payment Instrument, F.S. 831.28(a) – amend this statute to make the manufacturing / counterfeiting of a payment instrument a second degree felony with a offense severity ranking of seven;
2. Criminal Use of Personal Identification Information, F.S. 817.568(1)(d) – amend the definition of individual to include a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity;
3. Federal Law Enforcement Officers, Powers, F.S. 901.1505(2) – amend this statute to give federal law enforcement officers peace officer status / arrest powers for crimes enumerated under Chapter 817 and 831;

Statutory Enactments

1. Create a statute setting standards for businesses for the safeguard and disposal of personal identification information. At a minimum this statute should include a requirement that businesses shred or destroy documents that contain personal identification information as defined under F.S. 800;
2. Create a statute that provides an identity theft enhancement. Specifically, a statute that provides if during the commission of a felony an individual uses the personal identification information of another person the felony is reclassified one degree;

Florida Highway Patrol (FHP) / Department of Highway Safety Motor Vehicle

1. Provide funding for the purchase of facial recognition software for use by the FHP / DHSMV in determining victims of identity theft;
2. Provide funding for the placement of Troopers at DMV Offices;

Law Enforcement Training

1. The Florida Department of Law Enforcement (FDLE) is tasked with setting the mandatory training requirements in order for an individual to become a certified law enforcement officer in this state. This training should be amended to include a block of instruction on the investigation of identification theft crimes;
2. The FDLE Computer Division provide training on the investigation of computer related crimes. This training is primarily focused on law enforcement. An outreach program specifically targeting Prosecutors throughout the state would provide more Prosecutors with the requisite knowledge to handle these types of cases;

State Attorney's Office

1. Enact a legislative mandate that requires each SAO to designate two Assistant State Attorney's as "identity theft" Prosecutors. This would ensure each judicial circuit has subject matters experts that can assist both law enforcement and victims of identity theft.

During the course of my testimony members of your committee requested information on two additional issues involving the DHSMV. Specifically, what percentage of funding, if any, does the DHSMV receive from the Federal government for the purpose of developing tamper proof drivers licenses (DL) / identification (ID) cards. My agency was unable to find any specific data related to this question. The DHSMV may be able to provide information related to this inquiry.

Secondly, there was a discussion as to whether there is any type of audit process for the DHSMV Offices, Tax Collector's Office, and other offices that issue DL / ID Cards. The Florida Highway Patrol conducts "security assessment" on offices that issue DL / ID Cards. These "security assessments" audit whether the office is properly following guidelines for the issuance of DL / ID Cards. The FHP / DHSMV should be able to provide further information regarding the results of these "security assessments."

Finally, after my testimony I received a call from Sandra Lambert, Director of the Division of Driver Licenses. Ms. Lambert disagreed with much of my testimony regarding the problems I described regarding identity theft and drivers licenses. Among other issues she indicated there are overtime funds to place law enforcement in DMV Offices as a deterrent to criminals and the facial recognition software was utilized for a specific project. It was not specifically considered for purchase for wholesale use throughout the DMV. In order to ensure your committee receives the most complete information possible I wanted to make you aware of my discussion with

Ms. Lambert. Thank you for this opportunity to assist your committee.

Sincerely,

Kevin C. Frein

Kevin C. Frein
Assistant State Attorney

831.28 Counterfeiting a payment instrument; possessing a counterfeit payment instrument; penalties.—

(1) As used in this section, the term "counterfeit" means the manufacture of or arrangement to manufacture a payment instrument, as defined in s. 560.103, without the permission of the financial institution, account holder, or organization whose name, routing number, or account number appears on the payment instrument, or the manufacture of any payment instrument with a fictitious name, routing number, or account number.

(2)(a) *It is unlawful to counterfeit a payment instrument with the intent to defraud a financial institution, account holder, or any other person or organization or for a person to have any counterfeit payment instrument in such person's possession. Any person who violates this subsection commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.*[1]

(b) The printing of a payment instrument in the name of a person or entity or with the routing number or account number of a person or entity without the permission of the person or entity to manufacture or reproduce such payment instrument with such name, routing number, or account number is prima facie evidence of intent to defraud.

(3) This section does not apply to a law enforcement agency that produces or displays counterfeit payment instruments for investigative or educational purposes.

History.—s. 14, ch. 2001-115.

---

[1] A felony of the third degree is punishable by a term of imprisonment not to exceed 5 years and a fine not to exceed $5,000. A felony of the second degree is punishable by a term of imprisonment not to exceed 15 years and a fine not to exceed $10,000.

MISCELLANEOUS RECOMMENDATIONS:

NON-STATUTORY RECOMMENDATIONS

- Recommend to the Speaker that staff of the appropriate standing committee or of the Office of Program Policy and Government Accountability review, during the interim, state agency forms to determine the types of personal information collected by agencies.

- Recommend to the Speaker that staff of the appropriate standing committee study, during the interim, the issue of identity theft with a specific focus on the types of personal information commonly used by identity thieves to commit identity theft.

- Recommend to the Speaker and the Speaker-Designate that the Select Committee to Protect Personal Information be reestablished to continue reviewing the issues surrounding agency collection of information and the storage, retrieval, security, and destruction practices by agencies.

STATUTORY RECOMMENDATIONS

- Amend chapter 119, F.S., to create minimum requirements for agencies to meet when destroying hard copy and electronic public records containing confidential, exempt, or personal information.

- Amend chapter 119, F.S., to create a policy agencies must use when determining whether to actively publish public records on the Internet.