

**ALASKA STATE LEGISLATURE**  
**SENATE STATE AFFAIRS STANDING COMMITTEE**

January 29, 2009  
9:00 a.m.

**MEMBERS PRESENT**

Senator Linda Menard, Chair  
Senator Kevin Meyer, Vice Chair  
Senator Hollis French  
Senator Albert Kookesh  
Senator Joe Paskvan

**MEMBERS ABSENT**

All members present

**COMMITTEE CALENDAR**

SENATE BILL NO. 36

"An Act relating to the security of certain data processing records of the executive branch and making the Department of Administration responsible for the security of those records."

MOVED CSSB 36(STA) OUT OF COMMITTEE

**PREVIOUS COMMITTEE ACTION**

BILL: SB 36

SHORT TITLE: EXECUTIVE BRANCH RECORDS SECURITY

SPONSOR(S): SENATOR(S) THERRIAULT

01/21/09	(S)	PREFILE RELEASED 1/9/09
01/21/09	(S)	READ THE FIRST TIME - REFERRALS
01/21/09	(S)	STA, FIN
01/29/09	(S)	STA AT 9:00 AM BELTZ 211

**WITNESS REGISTER**

SENATOR GENE THERRIAULT  
Alaska State Legislature  
Juneau AK

**POSITION STATEMENT:** Presented SB 36 as sponsor.

ED SNIFFEN, Assistant Attorney General  
Department of Law  
Anchorage AK

**POSITION STATEMENT:** Spoke in support of SB 36.

KEVIN BROOKS, Deputy Commissioner  
Department of Administration  
Juneau AK

**POSITION STATEMENT:** Spoke in support of SB 36.

PAT DAVIDSON, Auditor  
Division of Legislative Audit  
Juneau AK

**POSITION STATEMENT:** Spoke in support of SB 36.

#### **ACTION NARRATIVE**

[9:00:45 AM](#)

**CHAIR LINDA MENARD** called the Senate State Affairs Committee meeting to order at 9:00 a.m. Senators French, Paskvan, and Menard were present at the call to order. Senator Meyer joined the committee soon thereafter. Senator Kookesh arrived later.

#### **SB 36-EXECUTIVE BRANCH RECORDS SECURITY**

CHAIR MENARD announced the consideration of SB 36.

[9:01:20 AM](#)

SENATOR FRENCH moved to adopt the committee substitute (CS) to SB 36 [labeled 26-LS0232\E], as a working document. Hearing no objection, Version E was before the committee.

SENATOR GENE THERRIAULT, Alaska State Legislature, Sponsor of SB 36, said he has been involved in identity theft legislation before. There was comprehensive legislation passed last year, and SB 36 is the next step in assuring Alaska citizens that data collected by private businesses and the state government is protected. He said he requested an audit a couple of years ago regarding identity theft and private businesses, but he became concerned because the state was Alaska's largest data collector. He wanted Alaska to give citizens the same protections required by the private sector. He requested an audit and found that the state did need work on that issue. This legislation includes recommendations from the auditor and from the Department of Administration (DOA). The intent is to strengthen the statutes and clarify that the duty and responsibility for security standards lies within the DOA. The DOA will have the authority to set the security policy and monitor the implementation and adherence to it by the different executive branches. The DOA will have the power to review and report the effectiveness of

the policy. There are state and federal laws that require citizens to give personal information to the government, and how that information is protected is a great concern.

[9:04:49 AM](#)

SENATOR THERRIAULT said the definition of "personally identifiable information" (PII) is "when you have a name, an address, a phone number, and it's combined with a social security number, Alaska driver's license number, or another I.D. number, credit card number, debit card number, account password, or P.I.N. ... or different combinations of those bits of information is what can be used by a scammer or an identity thief to take over somebody's identity and cause the economic damage." State systems gathering that data relate to workers compensation, unemployment insurance, child support, permanent fund dividends, driver's licenses, student loans, fish and game information, teacher certification files, retirement, payroll, health insurance, occupational licensing, voter registration, and others. There are about 642 information systems within state government that capture that kind of data, and over 200 capture the information that meet the definition of PII.

[9:06:26 AM](#)

SENATOR THERRIAULT said Section 1 of SB 36 is largely conforming. It tells the state archivist what information he or she has and how to treat it. The archivist would have to follow that new statute. Section 2 refers to the duties of the chief executive officer for the state. It adds language to an existing set of statutes to be subject to the new section that the bill creates. Section 3 is the new language, and it clarifies that the commissioner of administration is the chief information officer for the state. Section 4 refers to how the security records are handled and protected.

[9:07:58 AM](#)

SENATOR KOOKESH arrived.

SENATOR MEYER asked how the policy will be enforced through all the different agencies.

SENATOR THERRIAULT said he would like to see a set of standards, and the commissioner of DOA will set the policies. "We're not leaving it up to each agency and each division to come up with what records they think need to be protected, how they think they need to be protected. We're looking for standardization across all the agencies." The DOA will work with the agencies,

and there will be periodic reports back to the legislature to assess if agencies are meeting the standards.

9:09:55 AM

SENATOR MEYER asked if the reports will be annual.

SENATOR THERRIAULT said Section 5 requires the first report to be due on January 1 of the fifth calendar year after the act takes effect. Page 4, line 19, states that the legislature will then get a report every two years. It would give agencies quite a bit of time to come up to the standard that is set.

9:10:46 AM

SENATOR PASKVAN asked how long it will take to write the regulations.

9:11:30 AM

ED SNIFFEN, Assistant Attorney General, Department of Law, Anchorage, said regulations generally take six months to a year.

KEVIN BROOKS, Deputy Commissioner, Department of Administration, Juneau, said a "reg package is not a short process." But the DOA would not need it to proceed with many of the things in the bill and to continue with ongoing efforts with security.

9:12:53 AM

SENATOR FRENCH asked Mr. Brooks about the department's perspective on SB 36.

MR. BROOKS said DOA supports the legislation. It is a logical progression from House Bill 65 of 2008. Security of data that the state collects has been at the forefront for a number of years. The legislature has appropriated money to DOA to strengthen the security systems. He said he worked with the sponsor to clarify the language. "The state's I.T. [information technology] infrastructure didn't just occur, it's been incremental over the last 20 or so years or more." There are so many databases with each department responsible for the data, it is prudent to distinguish the commissioner of DOA to be the C.I.O. [chief information officer] for the state. The department has statutory authority over data processing and telecommunication. This will enable DOA to set standards and protocols for the state agencies. DOA has a state security office now, and it interacts with other states on security matters. The approach is good. There is a governance structure that includes the I.T. managers for each state agency. There are working groups that come together to discuss the best standards.

"The entire state has gone to a Microsoft exchange platform for state email, where we previously had five separate systems." There are groups functioning now, and SB 36 is a logical progression in that effort.

[9:15:19 AM](#)

SENATOR FRENCH asked if anything in the bill will cause the separate data silos to be integrated any better. He is interested in increasing the ability for those databases to talk to one another.

MR. BROOKS said the bill doesn't require that, but that effort is ongoing. "If you're going to do a database you need to use a sequel-server database or an oracle database, so the efforts are in place now to really get that integration." An earlier version of the bill could have been read to have the state build a super data farm and put all of its servers in one place. If the state were starting today, that may be the approach, "but recognizing that we have servers and data repositories all over the state in all departments, I think this is a prudent approach."

[9:16:34 AM](#)

SENATOR FRENCH asked if there have been breaches to the database by hackers.

MR. BROOKS said there have been, and everyday there are attempts. There was a breach in February 2005, and that event brought focus to the issue. There has been a data explosion for the state, but there have not been severe breaches where personal data has gone out, but the attacks occur daily and are becoming more sophisticated. "We need to be diligent."

SENATOR PASKVAN asked if there is protocol to notify a person if there was a breach in his or her information.

MR. BROOKS said yes, and House Bill 65 of 2008 set those protocols in place.

[9:18:10 AM](#)

PAT DAVIDSON, Auditor, Division of Legislative Audit, Juneau, said she was asked by the Budget and Audit Committee to conduct an audit on state security issues as it relates to PII (personal identifiable information). It is the first of a two-part audit looking at the governance structure associated with state security. For the second phase, two individual systems were selected for additional testing. The recommendations in SB 36 are parallel to concerns of the audit division. The audit found

that the governance structure was not very strong. "The state security office was getting a little push-back from some of the departments with regard to establishing standards." Security goes across departmental silos. "You get in one place; you find the weakest access point; you get in and then you can wander around in there." If there is a weakness in one department, the database may be vulnerable in another department.

MS. DAVIDSON said this is an important statewide issue that needs to be dealt with on a comprehensive basis. Putting the DOA in charge is a good idea. The audit included "dumpster diving." Auditors went to the sixth floor of the state office building and a few other locations and saw that medical, payroll, and other records were left out for recycling. "We found astonishing things." More disturbing was that the agency "gave us blank looks, like ... 'what's the problem?'" So raising security awareness consciousness has to happen, and it needs to be statewide. The I.T. experts understand it very well, "but if you're talking to an administrative assistant who's just trying to gather up the recycling, they don't have that in the forefront of their consciousness. This has to be an integrated training process." Setting the standards and moving them forward is really important for state government.

[9:21:52 AM](#)

SENATOR FRENCH referred to the obligations required by SB 36 on page 4. It looks like the bill is focused on data processing records, and those are records that are produced by the automatic data processing resources. He asked if it would include the records in the recycling bins.

[9:22:51 AM](#)

MS. DAVIDSON said it will be a combination of both. Some are printouts from data that has been collected. "Payroll records are going to be paper output from the payroll system." Some will be emails. She found things that people put in emails that had a lot more information than should be. "As we were evaluating the state security office - discussion of that - again, I.T. folks know that that's important. And the more authority you vest in somebody, and responsibility, I think you're going to see that taken up as more of an issue -- maybe not directly as it's related here, because we are talking about just data processing records, but I think the security consciousness will start raising."

SENATOR FRENCH asked if the bill should be broader. This is the legislature's opportunity to tell administrative clerks not to

throw out a payroll record or an email. Line 26, Page 4, presents the idea most of "us" are worried about: records that include personally identifiable information. "That's really what we're trying to get at ... you're trying to keep those obviously, sort of, dangerous pieces of information about me or any other citizen from being put out in a recycle bin outside a state office."

[9:24:49 AM](#)

MS. DAVIDSON said that is a question for the sponsor. Laws might not be needed to raise the security consciousness, "you just need to put it into practice."

SENATOR MEYER said the original bill asked for an audit every two years, and the CS asks for a legislative report. He asked if Ms. Davidson will have to jump in a dumpster every two years to ensure compliance.

MS. DAVIDSON said the current version doesn't refer to an audit; it refers to an evaluation that will be done by DOA. The audit division will not do it.

[9:26:24 AM](#)

SENATOR MEYER said the original bill asked for an audit.

SENATOR THERRIault said the bill was changed from a rigorous audit that could take six to eight months to even begin and another year to complete. He wants the DOA to put together a report on how closely the policies are being followed. It does not preclude Legislative Budget and Audit from asking for a full-blown audit from outside of the executive branch. He didn't want that expense every two years.

SENATOR THERRIault referred to page 4, lines 2 and 3, which state, "state agency responsible for insuring the security of the non-archive records produced from those databases." So most of what was found in a recycle bin was produced from the electronic silos. He believes there is language that covers Senator French's concerns.

[9:28:56 AM](#)

SENATOR MEYER asked if the departments are expected to just absorb this work without any cost.

SENATOR THERRIault said the DOA prepared a zero fiscal note. As Mr. Brooks mentioned, the department has an ongoing effort. When House Bill 65 passed last year, it had a \$2 million fiscal note

for software and to work "in this direction." But it wasn't standardized across all agencies, and there was actually resistance from some agencies. The person in the transportation department won't know why medical records could be an issue, but penetration can come from the department and "the person can run amok within the state system."

[9:30:32 AM](#)

MR. SNIFFEN said the bill is a good effort. Identity theft has become a serious problem across the country, "and we see a lot of that in the consumer protection section that I work in." Any efforts to help secure this kind of information will go a long way. The legislation is a good idea.

[9:31:34 AM](#)

CHAIR MENARD said legislators can help by having office shredders and by trying to "do our part in our own personal senate offices."

[9:32:04 AM](#)

SENATOR PASKVAN moved to report the CS to SB 36 [26-LS0232\E] from committee with individual recommendations and accompanying fiscal notes. Hearing no objections, CSSB 36(STA) passed out of committee.

[9:32:38 AM](#)

There being no further business to come before the committee, the meeting was adjourned at 9:32 a.m.