HB

520

COMMITTEE REPORT

SENATE

FURTHER:

Date _____

Mr. President

The Committee on _____ considered _____

and (a majority of the committee) (the committee) reports it back with the following recommendations:

[ ] do pass

[ ] do pass with attached amendment(s)

[ ] replace with/or adopt CS for _____
[ ] new title
[ ] same title and recommends _____

[ ] and attached a "LETTER OF INTENT" [ ] NEW FISCAL NOTE

[ ] reports it back without recommendation

[ ] recommends referral to _____ Committee

MEMBERS SIGNING
DO PASS

_____

_____

_____

_____

_____

_____

_____

_____

MEMBERS HAVING
OTHER RECOMMENDATIONS

_____

_____

_____

_____

_____

_____

_____

_____

_____
Chairman

_____
Chairman recommendation

COMMITTEE REPORT

SENATE

FURTHER:

Date _____

Mr. President

The Committee on _____ considered _____

and (a majority of the committee) (the committee) reports it back with the following recommendations:

[ ] do pass

[ ] do pass with attached amendment(s)

[ ] replace with/or adopt CS for _____
[ ] new title
[ ] same title and recommends _____

[ ] and attached a "LETTER OF INTENT" [ ] NEW FISCAL NOTE

[ ] reports it back without recommendation

[ ] recommends referral to _____ Committee

MEMBERS SIGNING
DO PASS

_____

_____

_____

_____

_____

_____

_____

_____

MEMBERS HAVING
OTHER RECOMMENDATIONS

_____

_____

_____

_____

_____

_____

_____

_____
Chairman

_____
Chairman recommendation

FISCAL NOTE

Revision Date:

REQUEST

Bill/Resolution No.: HB 520
Title: "An Act relating to criminal use of a computer."
Sponsor: Repr. Hayes
Requestor: House Judiciary
Date of Request: 1/26/84

FISCAL DETAIL

Agency Affected: Department of Law
Program Category Affected: Admin. of Justice
BRU, Program or Subprogram(s) Affected: Prosecution

EXPENDITURES/REVENUES: (Thousands of Dollars)

OPERATING	FY 84	FY 85	FY 86	FY 87	FY 88	FY 89
100 PERSONAL SERVICES						
200 TRAVEL						
300 CONTRACTUAL						
400 SUPPLIES						
500 EQUIPMENT						
600 LAND & STRUCTURES						
700 GRANTS, CLAIMS						
800 MISCELLANEOUS						
TOTAL OPERATING	-0-	-0-	-0-	-0-	-0-	-0-
CAPITAL						
REVENUE						

FUNDING: (Thousands of Dollars)

GENERAL FUND	-0-	-0-	-0-	-0-	-0-	-0-
FEDERAL FUNDS						
OTHER						
TOTAL						

POSITIONS:

FULL-TIME	-0-	-0-	-0-	-0-	-0-	-0-
PART-TIME						
TEMPORARY						

SOURCE OF FUNDS TO OFFSET FISCAL IMPACT OF BILL:

N/A

ANALYSIS: Attach a separate page for analysis

Prepared By: Richard I. Peques, Director Phone: 465-3672
Division: Administrative Services Division Date: 2-1-84

Approved by Commissioner: Norman C. Gorsuch Date: 2-1-84
Agency: Department of Law

Distribution (by Agency preparing fiscal note):
- Legislative Finance
- Legislative Sponsor
- Requestor
- Office of Management and Budget
- Impacted Agency(ies)

12/1/83

Fiscal Note
Analysis
HB 520

February 1, 1984

This bill addresses a limited area of criminal activity where a person uses a computer system or a computer network to commit a crime. Because existing statutes already cover most of the criminal acts set out in the bill, enactment of this legislation will have little, if any, fiscal impact on the Department of Law's operations. This bill's provision making it a crime to use a computer to obtain information with no legal right to do so concerning the credit information of a person clarifies and strengthens existing law.

POSITION PAPER

HB 520

This bill defines certain elements of computer stored data as private and classifies attempts to access, use or modify that data as criminal acts.

The Department of Administration supports this bill as an aid and clarification to administering disciplinary action in the area of data security infringements.

A recent incident pointed out the necessity for clearer statutory instructions in the area of non-authorized data access. This bill represents a step toward clarifying those instructions and lays a base for future statutes if deemed necessary.

James R. Shea, Deputy Commissioner
Information Resource Management

1/26/84
Date

Lisa Rudd, Commissioner
Department of Administration

1/26/84
Date

A PRESENTATION ON

COMPUTER CRIME LEGISLATION

Prepared for

MEMBERS OF THE LEGISLATURE

THE STATE OF ALASKA

December, 1983

THE NEED FOR COMPUTER CRIME LEGISLATION

INTRODUCTION

Several issues related to the information services industry have led to the need for computer crime legislation.

The computer industry has created a consumer market that has put machines in the hands of hobbyists, and controls in the data processing industry have been reduced thru time-sharing options and other productional facets. While we see individuals invading systems in the news and entertainment mediums, the point is being raised that it will not be long before true criminals are involved in other areas. Unfortunately, this has become a reality. Little publicity is given to these cases of computer crime because they are not always turned over to law enforcement agencies. This is because computer crime statutes, for the most part, are either not in place or insufficient to result in prosecution. With little chance of achieving successful prosectution, or even getting to court, it is not surprising that many companies do not report computer crime.

Because of growing problems and concerns about unauthorized access to and manipulation of computer-based information, it is necessary to enact legislation. After unsuccessful attempts at the national level, it has become necessary to have progressive state legislatures implement legislation on a state-by-state basis.

UNAUTHORIZED ACCESS TO CREDIT INFORMATION

The credit industry has evidenced criminal behavior thru unauthorized access in three basic scenarios:

1. Consumer victimization via stolen access codes.

2. File manipulation.

3. Investigation and collection agency activity using stolen access codes.

Each of these scenarios is elaborated on separately to illustrate the impact of this activity and the need for up-to-date legislation.

Consumer Victimization

Attachment A, "For Sale: Credit Ratings," describes a process of victimization. The act of a consumer obtaining a good credit rating was facilitated by stealing subscriber access codes. The individuals that were selling these packages telephoned legitimate credit grantors subscribing to the credit agency. These individuals represented themselves as calling from the credit agency, usually using the pretext of clearing up a billing problem, or being from the security department. During the conversation the access code is requested and usually provided. This access code enables access to the credit data base to facilitate the process. The buyer of the good credit history uses the good accounts and requests other credit cards. The buyer runs up bills with no intent of paying. The good consumer is left with the issue of clearing up his or her credit history once it has been discovered that someone has used the individual's history.

File Manipulation

Attachment B illustrates the issue of file manipulation. File manipulation is achieved by bribing someone to modify the information contained in files within the bureau or subscriber's premises and the submission of false credit information.

Unfortunately, not all bureaus have controls to prevent this access and many incidents of information modification occur. Once the bad credit history is deleted or modified, the individual applies for new credit accounts. (Controls exist within the TRW system to prevent and/or isolate attempts of this type.)

Even if consumer victimization and file manipulation efforts are successful, most law enforcement agencies will not pursue the case until there has been a loss to a credit grantor.

Investigation and Collection Agency Activity (Attachment C)

Private investigators, lawyers, and repossession agents may, in isolated cases, have a legitimate purpose to access a credit data base; however, most of the major credit agencies do not allow these individuals to subscribe due to the control features required to monitor permissible access.
Unfortunately, there have been many cases where individuals wanting this information have either stolen access codes or derived the access code from credit profiles sent to them by other subscribers with the access code on them.

Some collection agencies have acquired access codes in a similar manner. Although collection agencies have legitimate reasons to access a credit bureau, and they are subscribers, some do not use their own access code. The stolen access code is often utilized to reduce costs and increase commissions and agency profits.

A GROWING PROBLEM

According to recent statistics (Modern Office Procedures - March 1983, "Defending Your Computer Room Against Disaster") the average bank robbery is less than $3,000. The average "white collar" embezzlement nets less than $30,000. But the average computer crime is estimated to exceed $600,000, with little chance of detection, prosecution or conviction.

Education has become a key element in the fight against this area of criminal activity, and the United States Department of Justice has opened a specialized four week computer fraud school for F.B.I. agents. The Department of Justice, Sacramento, California, operates a two week course specializing in the same subject. Other municipalities as well as private organizations are currently holding seminars to combat problem areas of detection.

The challenge is to actively prosecute computer crime suspects. A challenge in the sense that the current laws regulating computer access are extremely lacking. Following, are three examples of TRW incidents that illustrate the need for computer crime legislation:

Example #1

An organized ring of credit criminals was established in a large metropolitan area. Although this example was taken from the Western Region, there is an indication that an identical ring is operating in the Eastern Region. One member of the ring provided computer password information to another who used it to gain access to our system. The suspect then retrieved hundreds of credit reports. Through a relocation and file merge system, the suspect was able to alter negative credit information into what appeared to be a positive profile.

The fee charged for this service varied, however, it averaged about $600 per report. This particular case is being actively prosecuted at the writing of this report. The section selected for prosecution was 502 P.C. (California).

Example #2

A collection agency/private investigative firm gained access to computer password information on several Information Services Division subscribers. As such, unauthorized access was made into our system and a total of $65,000 worth of credits were applied for from various east coast subscribers. While working the investigation of this matter, several New York agencies were contacted and each declined investigative jurisdiction. Most felt that it was a civil or federal problem, in that no computer crime bill existed.

Subsequently, the F.B.I. was contacted and consented to continue the investigation. A suspect was identified and prosecution is being actively pursued.

Example #3

A coast-to-coast organized crime ring obtained several thousand blank credit cards. Later, they obtained illegal access into credit systems and retrieved thousands of credit profiles of potential victims. By viewing the reports, account number information was obtained and later embossed on the stolen cards. The total amount stolen from creditors is unknown at this time, but it is believed to exceed $1,000,000. Investigation is continuing.

Crimes by these individuals were made possible through the illegal access to computer files. In each case the criminal simply called a TRW operator and relinquished certain password information which then caused the computer to be accessed.

It is acutely apparent that much has been done in the area of detection, but legislation is now needed for active prosecution.

CALIFORNIA'S COMPUTER CRIME LEGISLATION

SB 648 (California Penal Code 502), of which a copy is attached, was introduced in the California Legislature in March of 1981. This bill modified the penal code to make it a crime to intentionally access or cause to be accessed any computer system or network for the purpose of damaging the credit rating of any person. The bill was sponsored by an individual in the San Diego District Attorney's office, Fraud Division, in response to a situation in San Diego in which an individual's credit file was sold for the purposes of obtaining credit under fraudulent circumstances. (Similar legislation has been enacted in New York.)

Legislative justification for the bill goes on to say:

> "The credit granting sector of private industry is being deluged with false and fraudulent applications for credit. It is not uncommon for individuals and organized groups to systematically apply for multiple credit cards, loans, etc. utilizing fictitious and false names, biographical information, and credit histories. These fraudulent applications are carefully created to fit within the credit grantors' criteria for issuance of credit - such policies which are well known to the applicants. Sophisticated wrinkles are added such as the use of telephone answering services, which have been provided a prepared script to read in case of inquiry by the credit granting agencies. The answering service tells the inquiring party 'that the applicant has been employed at a high salary for five years; that the applicant has successfully paid off a loan on a expensive automobile, etc.'
>
> Under existing law, the credit grantor must suffer a loss before this activity can be filed as a felony. This ridiculous posture does nothing to prevent repeated attempts to obtain credit by fraudulent means. It is likewise discouraging to the credit grantors, who having discovered these activities, bring them to the attention of law enforcement and discover that this conduct is at most a misdemeanor. (Section 532a, California Penal Code)"

ONE STEP TOWARD A SOLUTION

Because of the tremendous growth in computer-based information services and concerns about the unauthorized access to and abuse of this information, it is necessary to adopt legislation. It has become clear that a national computer crime bill has little chance of passage. Some states, though, have passed legislation in this area, and, it is hoped that similar legislation can be passed in other states to facilitate interstate criminal prosecution and standardize penalties.

TRW's Information Services Division is prepared to support your state's activities to enact needed computer crime legislation. We recommend adopting statues similar to those enacted in the States of California and New York (California's statute is attached).

11/1983

CALIFORNIA PENAL CODE - SUBSECTION 502

Definitions; computer system or network; intentional access to defraud or extort, or to obtain money, property or services with false or fraudulent intent, representations or promises; malicious access, alteration, deletion or damage; violations; penalty

(a) For purposes of this section:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

(2) "Computer system" means a machine or collection of machines, excluding pocket calculators which are not programmable and capable of being used in conjuction with external files, one or more of which contained computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(3) "Computer network" means an interconnection of two or more computer systems.

(4) "Computer program" means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.

(6) "Financial instrument" includes, but is not limited to, any draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(7) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(8) "Service" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses or causes to be accessed any computer system or computer network for the purpose of obtaining unauthorized information concerning the credit information of another person or who introduces or causes to be introduced false information into that system or network for the purpose of wrongfully damaging or wrongfully enhancing the credit rating of any person shall be guilty of a public offense.

(d) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

*** (e) Any person who violates the provisions of subdivision (b) ***, (c), or (d) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5000), or by imprisonment in the state prision for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

*** (f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction.

auditors commended Sandia's corrective actions and stated that it appeared that the problems had been solved. However, it would not pay those responsible for the laboratory to become complacent. Without continual policing, the problem will return. The auditors recommended periodic random sampling of computer files to check on unauthorized use of the system.

For Sale: Credit Ratings

While evidence is still not clear, it seems possible that a data theft gang has been operating in southern California. It appears that the ring has allowed those with poor credit ratings to use someone else's good rating as the basis for opening charge accounts and obtaining loans.

The crime apparently involved unauthorized access to a credit bureau data base to obtain financial information about individuals with a clean credit history. Good credit ratings are sold to people who have problems obtaining credit. The bad credit risk purchases information that will allow him to assume for credit purposes the identity of someone who has the same name but a better financial record. Information supplied includes such things as social security number, bank account number, and driver's license number.

This suspected crime came to light when an individual with a good credit rating became aware that his identity was being used by another. He contacted a number of different law enforcement agencies and informed them about the alleged crime. To date, investigative efforts have been hampered by the fact that, although everyone acknowledges that a crime has indeed taken place, no one has been able to figure out who has jurisdiction. Meanwhile, a number of questions remain unanswered:

- How was the data obtained from the supposedly secure files of the credit bureau?
- Who obtained the data?
- Is it an inside job?

These questions will remain unanswered until jurisdiction problems can be ironed out and further information developed.

Student Cracks School District's Computer System

A high school senior in Tucson, Arizona was successful in breaking into the school district's computer system. However, he is beginning to have regrets about his actions. Since his successful intrusion, security measures have been tightened, and his access to the computer has been reduced.

The student, Joel Snyder, first realized that he could break the system's security code when he was accessing the computer through a remote job entry terminal at his high school. He was quoted as saying that anyone with a knowledge of assembly language could easily circumvent the system's security features. The passwords protecting student grades and other information were unimaginative.

His attempt to gain access to another user's password was successful. As a result, Snyder felt he should inform the authorities about the security risks involved. However, officials tended to doubt that Joel Snyder had actually cracked the system. They were willing to acknowledge that he had obtained access to passwords, but they were never sure how he had done it.

In his attempt to publicize the security weakness, Joel appeared at a school board meeting and brought the matter to the attention of the board. This action had some results. System security was soon tightened. Students are now allowed to access the system only from RJE stations (not by dialing up from a modem), only during certain hours, and only while a teacher is present.

While he has proven that he has more than a passing knowledge of computers and their security features, Snyder does not plan a career in data processing. His first college choice is Stanford University, where he plans to major in liberal arts.

Although Joel Snyder's reasons for breaking security were not malicious, his action shows the ease with which intelligent students can circumvent security features in today's systems. Obviously, there are basic weaknesses in most security provisions.

SEP 3 1976

U.S. Charges Six Fixed Reports On Credit-Risk Buyers For Fee, Fed False Data Into Computers

Authorities Believe Plot May Have Led To Millions Of Dollars In Unpaid Bills

LOS ANGELES (AP) —With the aid of a file clerk, six men sought out persons with poor credit records and for fees of up to $1,500 improved their credit reports in the computer banks of the country's largest consumer credit bureau, a federal indictment charges.

The credit records were kept in the computers of TRW Credit Data in Anaheim, Calif. The company maintains credit files on about 50 million Americans living in 20 cities.

The files are used by banks, credit card companies, and other businesses seeking information concerning the credit worthiness of customers.

Authorities said the alleged scheme may have produced millions of dollars in unpaid bills and caused untold legal problems for firms that rely on credit information.

The six men are charged with conspiracy in the indictment returned Thursday by a grand jury. All six also are charged with at least one count of making false loan-application statements.

A TRW Credit Data file clerk, Kathleen Bennett, was named as an unindicted co-conspirator. Federal authorities said she is to be a government witness.

According to the indictment, Miss Bennett was paid $50 each time she improved the computerized credit records of people solicited by the ring.

Some Information Deleted

This allegedly was done by deleting bad payment records, information about bankruptcies, and other unfavorable material. In some cases, material indicating a good credit history was inserted, authorities said.

The indictment lists 26 persons who paid between $300 and $1,500 to have their credit records altered, but authorities said as many as 150 persons may have paid for such falsifications between August, 1974, and March, 1975.

With their improved credit records, these people obtained banks loans, credit cards, and credit at retail stores, authorities said, and many of them subsequently defaulted on payments.

FBI agents uncovered the plot and broke up the ring 18 months ago, authorities said. It took the FBI, a Justice Department Organized Crime Strike Force, and the U.S. Attorney's office nearly 1½ years to obtain the evidence needed to present the case to a grand jury.

Seven Counts In Indictment

Charged in the seven-count indictment were Philip Kostoff, 31, the alleged ringleader; his brother, Paul Kostoff, 33; Ronald C. Rossi, 41; John R. Dubbs, 41, Kenneth L. Stevenson, 39, and Sean Shanahan, 45. All live in Orange County, where Anaheim is located.

The indictment alleged that Philip Kostoff hired the other defendants to locate persons who wanted their credit ratings improved and also recruited Miss Bennett.

Authorities said TRW Data Credit, a division of Cleveland-based TRW, Inc., cooperated in the investigation and is lightening its security.

Authorities seize stolen computer reports

ORANGE — Detectives, armed with search warrants, last week seized several thousand credit reports that were allegedly stolen from TRW computers in Orange.

The records were seized by police during raids at three Los Angeles area companies — H.E.L.P. Locksmiths of Van Nuys, Searchers Investigations and Searchers Security Co., Los Angeles.

Police said entry into TRW's computer bank was made via telephone and teleprinters, using that company's codes.

No charges were filed against the officers of the three companies.

The search warrants served Thursday and Friday culminated a three-month investigation into what police said is "to the best of our knowledge, the first known reported crime of this particular type in California and the country."

Gil Hamblet, TRW's vice president of industry and public affairs, said the company first noticed the illegal access to their computer records six months ago.

He said the material relates to the pay habits of Southern California residents and does not include any other personal information, except their names, addresses and previous addresses.

The Van Nuys firm is an automobile repossession company and the two Los Angeles companies are private investigators who work for attorneys and corporations.

"Such records are used to obtain credit information on individuals," Detective John Carson said. "The records are also used in skip tracing."

Carson said the material is now being inventoried, and it will probably be a week before the police and the district attorney will be ready to file charges.

3 Firms Probed in Theft Of TRW Computer Data

Two Los Angeles private detective agencies and a Van Nuys vehicle repossession firm have been accused of illegally obtaining credit information from computers at TRW, Orange County authorities said Tuesday.

Police said the three firms gained access to the TRW records credit reporting agency's computer by using the codes issued to TRW subscribers. No dollar value has been set on the alleged theft.

Investigators said Tuesday that H.E.L.P. Locksmiths, the repossession company, had been using the codes of two Los Angeles Searchers and Searchers Security Co. investigations, the detective agencies, had been using them since 1977, police said.

Orange police Detective Roger Braham said that charges have been filed, but investigators are continuing thousands of records—mostly computer printouts—seized from the three firms in raids last week.

Gil Hamblet, vice president of public affairs for TRW's Information Services Division in Orange, said the firm's computer security surveillance system first spotted the illegal information requests entering in January.

Officials of the three companies that allegedly obtained the information illegally could not be reached for comment Tuesday.

APR 6 1982

Authorities seize stolen computer reports

ORANGE — Detectives, armed with search warrants, last week seized several thousand credit reports that were allegedly stolen from TRW computers in Orange.

The records were seized by police during raids at three Los Angeles area companies — H.E.L.P. Locksmiths of Van Nuys, Searchers Investigations and Searchers Security Co., Los Angeles.

Police said entry into TRW's computer bank was made via telephone and teleprinters, using that company's codes.

No charges were filed against the officers of the three companies.

The search warrants served Thursday and Friday culminated a three-month investigation into what police said is "to the best of our knowledge, the first known reported crime of this particular type in California and the country."

Gil Hamblet, TRW's vice president of industry and public affairs, said the company first noticed the illegal access to their computer records six months ago.

He said the material relates to the pay habits of Southern California residents and does not include any other personal information, except their names, addresses and previous addresses.

The Van Nuys firm is an automobile repossession company and the two Los Angeles companies are private investigators who work for attorneys and corporations.

"Such records are used to obtain credit information on individuals," Detective John Carson said. "The records are also used in skip tracing."

Carson said the material is now being inventoried, and it will probably be a week before the police and the district attorney will be ready to file charges.

Los Angeles Times
LOS ANGELES CA
D. 1,000,455 S. 1,174,115

APR 7 1982

3 Firms Probed in Theft of TRW Computer Data

Two Los Angeles private detective agencies and a Van Nuys vehicle repossession firm have been accused of massive electronic theft of credit information from computers at TRW, Orange County authorities said Tuesday.

Police said the three firms gained access to the records of thousands credit reporting agency's computer by obtaining codes issued to TRW subscribers. No dollar value has been set on the alleged theft.

Investigators said Tuesday that H.E.L.P. Locksmiths, the repossession company, had been using the codes for six months. Searchers and Security and Searchers Investigations, the detective agencies, had been using them since 1972, police said.

Orange police Detective Roger Graham said no charges have been filed, but investigators are considering thousands of records—mostly computer printouts—seized from the three firms in raids last week.

Gil Hamblet, vice president of public affairs for TRW's Information Services Division in Orange, said the firm's own security surveillance system first spotted the illegal information request entries in January.

Officials of the three companies that allegedly obtained the information illegally could not be reached for comment Tuesday.

Audit concludes state computers are vulnerable

By KARIN DAVIES
Daily News reporter

JUNEAU — The state computer system is poorly protected against tampering by unauthorized individuals, a recently released state audit says.

Because the computer security system is inadequate, someone who puts his mind to it could play with state records — including personnel, payroll and permanent fund dividend files, said James Shea, Department of Administration deputy commissioner of information resource management.

The Department of Administration's lack of policies, procedures and standards for computer operations "leaves the system open to errors and inefficiencies," the Legislative Audit Division said.

"In the worst case, the absence of adequate access controls over production files could expose application systems to errors, fraud and sabotage," the audit said.

Anyone with a current state computer account can change, replace or delete backup programs for the central accounting system, the report said.

The department has asked the legislature for $280,000 in the 1984-85 budget year to beef up security systems for central state computers in Juneau and Anchorage, Shea said. The money would pay for a security system and two people to maintain it.

Shea said computer tampering has become a concern nationwide as "computer literacy" increases. Recently, a state employee was disciplined for gathering the information that would have allowed him to enter files that were off limits to him.

House Speaker Joe Hayes, R-Anchorage, recently introduced legislation making it a felony to use computers to illegally obtain or alter information, steal money or to defraud or deceive someone.

A better computer security system would cut down on the number of checks and audits of records that the state would have to perform, Shea said.

The department also plans to comply with suggestions that rules for operating the state computer system be written, distributed and enforced, Shea said.

Several other procedural corrections will be made as well, according to a department response to the audit.

Computer meddling leads state to ask for more security

ADN 12/23

The Associated Press

JUNEAU — Allegations that a state employee tampered with a computer in an effort to gain access to the names of permanent fund dividend recipients has prompted officials to request a new, $240,000 computer security system, a spokeswoman said Thursday.

Frances Rose, a public information officer with the state Department of Administration, said the employee's name would not be released because he was not charged with any crime.

"He was suspended for 15 days, reduced two steps in rank and had his security clearance lifted," she said.

"If he had been successful, I presume he would have been fired straight out."

The employee is accused of trying to "get information he did not need," or the names of permanent fund dividend recipients, she said.

"I guess he thought he would solicit things from people after they got their checks," Rose said.

"This is the first time this kind of thing has happened. ... It's straight out of 'War Games' (a film about computer tampering)."

A system of "passwords" had been used by the state to safeguard computer information, "but I guess it's not foolproof," she said.

"There's a recognized need that we have to beef up our security," she said.

"We have a proposal in the fiscal '85 budget that would fund the installation of a new computer security system.

"The one they have in mind would cost $240,000 and include creating a data security office and an officer to monitor computer use," Rose said.

Gayle Horetski, an assistant attorney general, said Thursday the case was not referred to the Department of Law so there was no criminal prosecution.

"Computer tampering is something of a gray area and we're working now on legislation that would tighten it up," she said.

FILE WITH HB 520

TO: Senator Bill Ray

FROM: Paula d. Scavera

DATE: March 26, 1984

RE: HB 520 (Finance) am

SECTION 1

Adds new language which establishes the crime of Theft of Services. The penalty level for a specific crime will depend on the value of the service used. (Attached is a value of crime, and level of penalty chart.)

SECTION 2

Adds to the crime of Criminal Mischief in the Third Degree, a class A misdemeanor, a person who has no right, to knowingly access a computer.

SECTION 3

Adds a new crime to existing law; Criminal Use of a Computer and makes that crime a Class C felony.

SECTION 4

Adds new defintions of "access", "computer", "computer network", "computer system", and "data".

SECTION 5

Amends the definition of "services" to include use of a computer, computer time, or a computer system or network.

THEFT OF SERVICES VALUE/LEVEL CHART

SECTION 1 CSHB 520(Finance) am

VALUE	CRIME	LEVEL	PENALTY
$0-49	Theft 4th°	B mis.	90 days/ $1,000
$50-499	Theft 3rd°	A mis.	1 year/ $5,000
$500-24,999	Theft 2nd°	C Felony	5 years/ $50,000
$25,000 or more	Theft 1st°	B Felony	10 years/$50,000