

SENATE BILL NO. 279

INTRODUCED BY KEATING, GAGE, JACOBSON, NEUMAN,
SIMON, FRITZ, BRADLEY, COBB

BY REQUEST OF THE LEGISLATIVE AUDIT COMMITTEE

IN THE SENATE

FEBRUARY 3, 1987 INTRODUCED AND REFERRED TO COMMITTEE
ON STATE ADMINISTRATION.

FEBRUARY 19, 1987 COMMITTEE RECOMMEND BILL
DO PASS AS AMENDED. REPORT ADOPTED.

FEBRUARY 20, 1987 PRINTING REPORT.

FEBRUARY 21, 1987 SECOND READING, DO PASS.

FEBRUARY 22, 1987 ENGROSSING REPORT.

FEBRUARY 23, 1987 THIRD READING, PASSED.
AYES, 49; NOES, 0.

TRANSMITTED TO HOUSE.

IN THE HOUSE

FEBRUARY 24, 1987 INTRODUCED AND REFERRED TO COMMITTEE
ON STATE ADMINISTRATION.

MARCH 11, 1987 COMMITTEE RECOMMEND BILL BE
CONCURRED IN. REPORT ADOPTED.

MARCH 14, 1987 SECOND READING, CONCURRED IN.

ON MOTION, REREFERRED TO COMMITTEE
ON APPROPRIATIONS.

MARCH 23, 1987 COMMITTEE RECOMMEND BILL BE
CONCURRED IN. REPORT ADOPTED.

MARCH 28, 1987 SECOND READING, CONCURRED IN.

MARCH 30, 1987 THIRD READING, CONCURRED IN.
AYES, 98; NOES, 0.

RETURNED TO SENATE.

IN THE SENATE

MARCH 31, 1987

RECEIVED FROM HOUSE.

SENT TO ENROLLING.

APRIL 2, 1987

SIGNED BY PRESIDENT.

IN THE HOUSE

APRIL 2, 1987

SIGNED BY SPEAKER.

IN THE SENATE

APRIL 2, 1987

DELIVERED TO GOVERNOR.

APRIL 7, 1987

RETURNED FROM GOVERNOR WITH
RECOMMENDED AMENDMENTS.

APRIL 9, 1987

SECOND READING, GOVERNOR'S RECOM-
MENDED AMENDMENTS CONCURRED IN.

APRIL 10, 1987

THIRD READING, GOVERNOR'S RECOM-
MENDED AMENDMENTS CONCURRED IN.

IN THE HOUSE

APRIL 15, 1987

SECOND READING, GOVERNOR'S RECOM-
MENDED AMENDMENTS CONCURRED IN.

APRIL 16, 1987

THIRD READING, GOVERNOR'S RECOM-
MENDED AMENDMENTS CONCURRED IN.

RETURNED TO SENATE.

IN THE SENATE

APRIL 16, 1987

RECEIVED FROM HOUSE.

SENT TO ENROLLING.

1 *Senate* BILL NO. *279*
 2 INTRODUCED BY *Heating up Jacobson*
 3 BY REQUEST OF THE LEGISLATIVE AUDIT COMMITTEE *Cobb*
 4 *Simon Kelly Bradley*

5 A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING FOR SECURITY
 6 OF DATA AND INFORMATION TECHNOLOGY RESOURCES; ESTABLISHING
 7 THE RESPONSIBILITIES OF STATE AGENCIES, THE BOARD OF
 8 REGENTS, THE SUPREME COURT, AND THE DEPARTMENT OF
 9 ADMINISTRATION; AND AMENDING SECTION 2-15-102, MCA."

10
 11 WHEREAS, data and information collected and maintained
 12 by state government are assets which require protection; and

13 WHEREAS, the increasing use of information technology
 14 in state government requires a systematic risk-management
 15 approach to minimize increased security threats to data and
 16 information technology resources; and

17 WHEREAS, it is desirable to create a greater awareness
 18 regarding the importance of security of state government
 19 data and information technology resources; and

20 WHEREAS, a recent audit of mainframe computer security
 21 indicated a lack of security over data processing equipment
 22 and procedures.

23
 24 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:
 25 Section 1. Section 2-15-102, MCA, is amended to read:

1 "2-15-102. Definitions. As used in this chapter, the
 2 following definitions apply:

3 (1) "Executive branch" means the executive branch of
 4 state government referred to in the Montana constitution,
 5 Articles III and VI.

6 (2) "Agency" means an office, position, commission,
 7 committee, board, department, council, division, bureau,
 8 section, or any other entity or instrumentality of the
 9 executive branch of state government.

10 (3) "Unit" means an internal subdivision of an agency,
 11 created by law or by administrative action, including a
 12 division, bureau, section, or department, and an agency
 13 allocated to a department for administrative purposes only
 14 by this chapter.

15 (4) "Data and information technology resources" means
 16 data processing mainframe, microcomputer hardware,
 17 peripherals, software, service supplies, personnel, facility
 18 resources, maintenance, training, or other related
 19 resources.

20 ~~(4)~~(5) "Department" means a principal functional and
 21 administrative entity, created by this chapter within the
 22 executive branch of state government; is one of the 20
 23 principal departments permitted under the constitution; and
 24 includes its units.

25 ~~(5)~~(6) "Department head" means a director, commission,



1 board, commissioner, or constitutional officer in charge of
2 a department created by this chapter.

3 {6}{7} "Director" means a department head specifically
4 referred to as a director in this chapter, and does not mean
5 a commission, board, commissioner, or constitutional
6 officer.

7 {7}{8} "Advisory capacity" means furnishing advice,
8 gathering information, making recommendations, and
9 performing such other activities as may be necessary to
10 comply with federal funding requirements and does not mean
11 administering a program or function or setting policy.

12 {8}{9} "Function" means a duty, power, or program,
13 exercised by or assigned to an agency, whether or not
14 specifically provided for by law.

15 {9}{10} "Quasi-judicial function" means an adjudicatory
16 function exercised by an agency, involving the exercise of
17 judgment and discretion in making determinations in
18 controversies. The term includes but is not limited to the
19 functions of interpreting, applying, and enforcing existing
20 rules and laws; granting or denying privileges, rights, or
21 benefits; issuing, suspending, or revoking licenses,
22 permits, and certificates; determining rights and interests
23 of adverse parties; evaluating and passing on facts;
24 awarding compensation; fixing prices; ordering action or
25 abatement of action; adopting procedural rules; holding

1 hearings; and any other act necessary to the performance of
2 a quasi-judicial function.

3 {10}{11} "Quasi-legislative function" generally means
4 making or having the power to make rules or set rates and
5 all other acts connected with or essential to the proper
6 exercise of a quasi-legislative function."

7 NEW SECTION. Section 2. Responsibilities of
8 departments. Each department head is responsible for
9 assuring an adequate level of security for all data and
10 information technology resources within his department and
11 shall:

12 (1) develop and annually update written internal
13 policies and procedures to assure security of data and
14 information technology resources. The internal policies and
15 procedures are confidential information and exempt from
16 public inspection, except that such information must be
17 available to the legislative auditor in performing his
18 postauditing duties.

19 (2) designate an information security manager to
20 administer the department's security program for data and
21 information technology resources;

22 (3) conduct and annually update a risk analysis to
23 determine security threats to data and information
24 technology resources. The risk-analysis information is
25 confidential and exempt from public inspection, except that

1 such information must be available to the legislative
2 auditor in performing his postauditing duties.

3 (4) implement appropriate cost-effective safeguards to
4 reduce, eliminate, or recover from the identified risks to
5 data and information technology resources;

6 (5) ensure that annual internal evaluations of the
7 security program for data and information technology
8 resources are conducted. The results of such internal
9 evaluations are confidential and exempt from public
10 inspection, except that such information must be available
11 to the legislative auditor in performing his postauditing
12 duties.

13 (6) include appropriate security requirements, as
14 determined by the department, in the written specifications
15 for the department's solicitation of data and information
16 technology resources;

17 (7) maintain an information technology plan, including
18 a general description of the existing security program and
19 future plans for assuring security of data and information
20 technology resources; and

21 (8) certify annually to the department of
22 administration that the security program for data and
23 information technology resources conforms with the standards
24 and guidelines developed by the department of
25 administration. A department that is unable to certify its

1 conformance shall give written notice to the department of
2 administration, stating the deficiencies and the reasons for
3 nonconformance.

4 NEW SECTION. Section 3. Responsibilities of
5 department of administration. The department of
6 administration is responsible for providing centralized
7 management and coordination of state policies for security
8 of data and information technology resources and shall:

9 (1) establish and maintain the minimum security
10 standards, rules, and regulations to implement [section 2],
11 including the physical security of central and backup
12 computer facilities consistent with these standards;

13 (2) establish guidelines to assist agencies in
14 identifying electronic data processing personnel occupying
15 positions of special trust or responsibility or sensitive
16 locations;

17 (3) establish rules and regulations for the exchange
18 of data between data centers or departments by hardwired or
19 nondedicated telecommunications to ensure that exchanges do
20 not jeopardize data security and confidentiality;

21 (4) coordinate and provide for a training program
22 regarding security of data and information technology
23 resources to serve governmental technical and managerial
24 needs;

25 (5) include appropriate security requirements in the

1 specifications for solicitation of state contracts for
2 procuring data and information technology resources; and

3 (6) upon request, provide technical and managerial
4 assistance relating to the security program.

5 NEW SECTION. Section 4. Responsibilities of board of
6 regents. The board of regents is responsible for assuring an
7 adequate level of security for data and information
8 technology resources, as defined in 2-15-102, within the
9 state university system. In carrying out this
10 responsibility, the board of regents shall, at a minimum,
11 address the responsibilities prescribed in [section 2].

12 NEW SECTION. Section 5. Responsibilities of supreme
13 court. The supreme court is responsible for assuring an
14 adequate level of security for data and information
15 technology resources, as defined in 2-15-102, within the
16 judicial branch. In carrying out this responsibility, the
17 supreme court shall, at a minimum:

18 (1) address the responsibilities prescribed in
19 [section 2]; and

20 (2) develop written minimum standards and guidelines
21 for the judicial branch to follow in developing its security
22 program.

23 NEW SECTION. Section 6. Codification instructions.

24 (1) Sections 2 and 3 are intended to be codified as an
25 integral part of Title 2, chapter 15, part 10, and the

1 provisions of Title 2, chapter 15, part 10, apply to
2 sections 2 and 3.

3 (2) Section 4 is intended to be codified as an
4 integral part of Title 2, chapter 15, part 15, and the
5 provisions of Title 2, chapter 15, part 15, apply to section
6 4.

7 (3) Section 5 is intended to be codified as an
8 integral part of Title 3, chapter 2, part 6, and the
9 provisions of Title 3, chapter 2, part 6, apply to section
10 5.

-End-

STATE OF MONTANA - FISCAL NOTE

Form BD-15

In compliance with a written request, there is hereby submitted a Fiscal Note for SB279, as introduced.

DESCRIPTION OF PROPOSED LEGISLATION:

An act providing for security of data and information technology resources; establishing the responsibilities of state agencies, the Board of Regents, the supreme court, and the Department of Administration; and amending section 2-15-102, MCA.

ASSUMPTIONS:

Section 2. Establishing the responsibilities of departments.

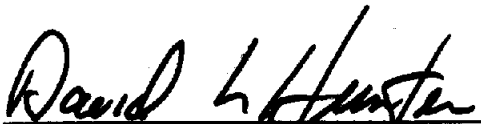
1. Department of Natural Resources and Conservation - funds remaining in building fund will cover the expenses of installation of a halon fire suppression system in the computer room and installation of a backup city water cooling system for the computer room air conditioner when the heat pump is not functioning.
2. There may be software, hardware or other as yet unknown resources needed to implement safeguards necessary to comply with an effective security program. The full extent of the resources needed will not be known until the risk analysis required by the bill has been completed.
3. Departments will be relying on Department of Administration for assistance.
4. Security recommendations made by the legislative auditor would correspond with those recommended by the Department of Administration.


Section 3. Establishing the responsibilities of the Department of Administration in setting rules, standards and agency training provisions.

1. Accommodation of bill requirements assumed to be completed in FY88, maintenance and revision of guidelines to continue in subsequent years.
2. Training program costs of \$12,840 for FY88 and \$5,860 for subsequent years assumes providing two security seminars annually; one addressing managerial security awareness, one emphasizing technical considerations for state agency personnel.
3. The costs shown are the additional costs needed to implement this legislation which expands the Department's security responsibilities.

Section 4. Establishing responsibilities of Board of Regents.

1. The campuses are currently doing some of the proposed activities outlined in the bill and can absorb internally some of the things they are currently not doing.
2. In order to fully address the areas that cannot be absorbed internally, 2 FTE's will have to be added to the University System.


DATE 2/9/87
DAVID L. HUNTER, BUDGET DIRECTOR
Office of Budget and Program Planning


DATE _____
THOMAS KEATING PRIMARY SPONSOR

Fiscal Note for SB279, as introduced.

SB 279

Section 5. Establishing responsibilities of supreme court.

1. There is no current staff available to establish and maintain written standards and guidelines. An FTE will need to be added.

NOTE: The information compiled in this fiscal note does not cover every agency. The larger agencies are represented, but some smaller agencies are not, due to the timing allowed for in processing fiscal notes.

FISCAL IMPACT:

Additional Cost:

	<u>FY88</u>	<u>FY89</u>
General Fund	\$ 79,461	\$ 28,206
Earmarked Special Revenue Fund	47,676	13,450
Federal and Private Special Revenue	235,200	84,000
Capitol Project Fund	0	0
Proprietary Fund	75,389	41,308
Current Unrestricted	45,000	45,000
Long-Range Building	8,500	0
Pension Trust	<u>2,964</u>	<u>700</u>
TOTAL	\$494,190	\$212,664

Funding for these costs are not currently in agency budgets.

LONG-RANGE EFFECTS OF PROPOSED LEGISLATION:

1. A maintenance of effort will need to be maintained in future years to allow for security in this area, due to changes in the field of data processing.

TECHNICAL OR MECHANICAL DEFECTS IN PROPOSED LEGISLATION OR CONFLICTS WITH EXISTING LEGISLATION:

N/A

APPROVED BY COMMITTEE
ON STATE ADMINISTRATION

SENATE BILL NO. 279

INTRODUCED BY KEATING, GAGE, JACOBSON, NEUMAN,

SIMON, FRITZ, BRADLEY, COBB

BY REQUEST OF THE LEGISLATIVE AUDIT COMMITTEE

A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING FOR SECURITY OF DATA AND INFORMATION TECHNOLOGY RESOURCES; ESTABLISHING THE RESPONSIBILITIES OF STATE AGENCIES, THE BOARD OF REGENTS, THE SUPREME COURT, AND THE DEPARTMENT OF ADMINISTRATION; AND AMENDING SECTION 2-15-102, MCA."

WHEREAS, data and information collected and maintained by state government are assets which require protection; and

WHEREAS, the increasing use of information technology in state government requires a systematic risk-management approach to minimize increased security threats to data and information technology resources; and

WHEREAS, it is desirable to create a greater awareness regarding the importance of security of state government data and information technology resources; and

WHEREAS, a recent audit of mainframe computer security indicated a lack of security over data processing equipment and procedures.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

Section 1. Section 2-15-102, MCA, is amended to read:
"2-15-102. Definitions. As used in this chapter, the following definitions apply:

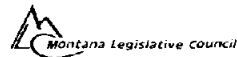
(1) "Executive branch" means the executive branch of state government referred to in the Montana constitution, Articles III and VI.

(2) "Agency" means an office, position, commission, committee, board, department, council, division, bureau, section, or any other entity or instrumentality of the executive branch of state government.

(3) "Unit" means an internal subdivision of an agency, created by law or by administrative action, including a division, bureau, section, or department, and an agency allocated to a department for administrative purposes only by this chapter.

(4) "Data and information technology resources" means data processing mainframe, microcomputer hardware, peripherals, software, ~~service--supplies~~ SPECIAL FORMS, personnel, facility resources, maintenance, training, ELECTRONICALLY STORED DATA, or other related resources.

(5) "Department" means a principal functional and administrative entity, created by this chapter within the executive branch of state government; is one of the 20 principal departments permitted under the constitution; and includes its units.



1 †5†(6) "Department head" means a director, commission,
2 board, commissioner, or constitutional officer in charge of
3 a department created by this chapter.

4 †6†(7) "Director" means a department head specifically
5 referred to as a director in this chapter, and does not mean
6 a commission, board, commissioner, or constitutional
7 officer.

8 †7†(8) "Advisory capacity" means furnishing advice,
9 gathering information, making recommendations, and
10 performing such other activities as may be necessary to
11 comply with federal funding requirements and does not mean
12 administering a program or function or setting policy.

13 †8†(9) "Function" means a duty, power, or program,
14 exercised by or assigned to an agency, whether or not
15 specifically provided for by law.

16 †9†(10) "Quasi-judicial function" means an adjudicatory
17 function exercised by an agency, involving the exercise of
18 judgment and discretion in making determinations in
19 controversies. The term includes but is not limited to the
20 functions of interpreting, applying, and enforcing existing
21 rules and laws; granting or denying privileges, rights, or
22 benefits; issuing, suspending, or revoking licenses,
23 permits, and certificates; determining rights and interests
24 of adverse parties; evaluating and passing on facts;
25 awarding compensation; fixing prices; ordering action or

1 abatement of action; adopting procedural rules; holding
2 hearings; and any other act necessary to the performance of
3 a quasi-judicial function.

4 †10†(11) "Quasi-legislative function" generally means
5 making or having the power to make rules or set rates and
6 all other acts connected with or essential to the proper
7 exercise of a quasi-legislative function."

8 NEW SECTION. Section 2. Responsibilities of
9 departments. Each department head is responsible for
10 assuring an adequate level of security for all data and
11 information technology resources within his department and
12 shall:

13 (1) develop and ~~annually--update~~ MAINTAIN written
14 internal policies and procedures to assure security of data
15 and information technology resources. The internal policies
16 and procedures are confidential information and exempt from
17 public inspection, except that such information must be
18 available to the legislative auditor in performing his
19 postauditing duties.

20 (2) designate an information security manager to
21 administer the department's security program for data and
22 information technology resources;

23 ~~(3)--conduct-and-annually-update-a--risk--analysis--to~~
24 ~~determine---security---threats---to---data--and--information~~
25 ~~technology--resources;--The--risk-analysis--information---is~~

1 ~~confidential--and-exempt-from-public-inspection,--except-that~~
 2 ~~such--information--must--be--available--to--the--legislative~~
 3 ~~auditor-in-performing-his-postauditing-duties.~~

4 ~~(4)(3)~~ implement appropriate cost-effective safeguards
 5 to reduce, eliminate, or recover from ~~the-identified-risks~~
 6 IDENTIFIED THREATS to data and information technology
 7 resources;

8 ~~(5)(4)~~ ensure ~~that-annual~~ internal evaluations of the
 9 security program for data and information technology
 10 resources are conducted. The results of such internal
 11 evaluations are confidential and exempt from public
 12 inspection, except that such information must be available
 13 to the legislative auditor in performing his postauditing
 14 duties.

15 ~~(6)(5)~~ include appropriate security requirements, as
 16 determined by the department, in the written specifications
 17 for the department's solicitation of data and information
 18 technology resources; AND

19 ~~(7)(6)~~ maintain an information technology plan,
 20 including a general description of the existing security
 21 program and future plans for assuring security of data and
 22 information technology resources; and,

23 ~~(8)--certify--annually--to--the--department--of~~
 24 ~~administration--that--the--security--program--for--data--and~~
 25 ~~information-technology-resources-conforms-with-the-standards~~

1 ~~and---guidelines---developed---by---the---department---of~~
 2 ~~administration.--A-department-that-is-unable-to--certify--its~~
 3 ~~conformance--shall--give-written-notice-to-the-department-of~~
 4 ~~administration,--stating-the-deficiencies-and-the-reasons-for~~
 5 ~~nonconformance.~~

6 NEW SECTION. Section 3. Responsibilities of
 7 department of administration. The department of
 8 administration is responsible for providing centralized
 9 management and coordination of state policies for security
 10 of data and information technology resources and shall:

11 (1) establish and maintain the minimum security
 12 standards, ~~rules,--and-regulations~~ AND POLICIES to implement
 13 [section 2], including the physical security of central and
 14 backup computer facilities consistent with these standards;

15 (2) establish guidelines to assist agencies in
 16 identifying electronic data processing personnel occupying
 17 positions of special trust or responsibility or sensitive
 18 locations;

19 (3) establish ~~rules--and--regulations~~ STANDARDS AND
 20 POLICIES for the exchange of data between data centers or
 21 departments by hardwired or nondedicated telecommunications
 22 to ensure that exchanges do not jeopardize data security and
 23 confidentiality;

24 (4) coordinate and provide for a training program
 25 regarding security of data and information technology

1 resources to serve governmental technical and managerial
2 needs;

3 (5) include appropriate security requirements in the
4 specifications for solicitation of state contracts for
5 procuring data and information technology resources; and

6 (6) upon request, provide technical and managerial
7 assistance relating to the security program.

8 NEW SECTION. Section 4. Responsibilities of board of
9 regents. The board of regents is responsible for assuring an
10 adequate level of security for data and information
11 technology resources, as defined in 2-15-102, within the
12 state university system. In carrying out this
13 responsibility, the board of regents shall, at a minimum,
14 address the responsibilities prescribed in [section 2].

15 NEW SECTION. Section 5. Responsibilities of supreme
16 court. The supreme court is responsible for assuring an
17 adequate level of security for data and information
18 technology resources, as defined in 2-15-102, within the
19 judicial branch. In carrying out this responsibility, the
20 supreme court shall, at a minimum:

21 (1) address the responsibilities prescribed in
22 [section 2]; and

23 (2) develop written minimum standards and guidelines
24 for the judicial branch to follow in developing its security
25 program.

1 NEW SECTION. Section 6. Codification instructions.

2 (1) Sections 2 and 3 are intended to be codified as an
3 integral part of Title 2, chapter 15, part 10, and the
4 provisions of Title 2, chapter 15, part 10, apply to
5 sections 2 and 3.

6 (2) Section 4 is intended to be codified as an
7 integral part of Title 2, chapter 15, part 15, and the
8 provisions of Title 2, chapter 15, part 15, apply to section
9 4.

10 (3) Section 5 is intended to be codified as an
11 integral part of Title 3, chapter 2, part 6, and the
12 provisions of Title 3, chapter 2, part 6, apply to section
13 5.

-End-

1 SENATE BILL NO. 279

2 INTRODUCED BY KEATING, GAGE, JACOBSON, NEUMAN,

3 SIMON, FRITZ, BRADLEY, COBB

4 BY REQUEST OF THE LEGISLATIVE AUDIT COMMITTEE

5
6 A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING FOR SECURITY
7 OF DATA AND INFORMATION TECHNOLOGY RESOURCES; ESTABLISHING
8 THE RESPONSIBILITIES OF STATE AGENCIES, THE BOARD OF
9 REGENTS, THE SUPREME COURT, AND THE DEPARTMENT OF
10 ADMINISTRATION; AND AMENDING SECTION 2-15-102, MCA."

11
12 WHEREAS, data and information collected and maintained
13 by state government are assets which require protection; and

14 WHEREAS, the increasing use of information technology
15 in state government requires a systematic risk-management
16 approach to minimize increased security threats to data and
17 information technology resources; and

18 WHEREAS, it is desirable to create a greater awareness
19 regarding the importance of security of state government
20 data and information technology resources; and

21 WHEREAS, a recent audit of mainframe computer security
22 indicated a lack of security over data processing equipment
23 and procedures.

24
25 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

1 Section 1. Section 2-15-102, MCA, is amended to read:

2 "2-15-102. Definitions. As used in this chapter, the
3 following definitions apply:

4 (1) "Executive branch" means the executive branch of
5 state government referred to in the Montana constitution,
6 Articles III and VI.

7 (2) "Agency" means an office, position, commission,
8 committee, board, department, council, division, bureau,
9 section, or any other entity or instrumentality of the
10 executive branch of state government.

11 (3) "Unit" means an internal subdivision of an agency,
12 created by law or by administrative action, including a
13 division, bureau, section, or department, and an agency
14 allocated to a department for administrative purposes only
15 by this chapter.

16 (4) "Data and information technology resources" means
17 data processing mainframe, microcomputer hardware,
18 peripherals, software, ~~service-supplies~~ SPECIAL FORMS,
19 personnel, facility resources, maintenance, training,
20 ELECTRONICALLY STORED DATA, or other related resources.

21 (5) "Department" means a principal functional and
22 administrative entity, created by this chapter within the
23 executive branch of state government; is one of the 20
24 principal departments permitted under the constitution; and
25 includes its units.

1 {5}(6) "Department head" means a director, commission,
 2 board, commissioner, or constitutional officer in charge of
 3 a department created by this chapter.

4 {6}(7) "Director" means a department head specifically
 5 referred to as a director in this chapter, and does not mean
 6 a commission, board, commissioner, or constitutional
 7 officer.

8 {7}(8) "Advisory capacity" means furnishing advice,
 9 gathering information, making recommendations, and
 10 performing such other activities as may be necessary to
 11 comply with federal funding requirements and does not mean
 12 administering a program or function or setting policy.

13 {8}(9) "Function" means a duty, power, or program,
 14 exercised by or assigned to an agency, whether or not
 15 specifically provided for by law.

16 {9}(10) "Quasi-judicial function" means an adjudicatory
 17 function exercised by an agency, involving the exercise of
 18 judgment and discretion in making determinations in
 19 controversies. The term includes but is not limited to the
 20 functions of interpreting, applying, and enforcing existing
 21 rules and laws; granting or denying privileges, rights, or
 22 benefits; issuing, suspending, or revoking licenses,
 23 permits, and certificates; determining rights and interests
 24 of adverse parties; evaluating and passing on facts;
 25 awarding compensation; fixing prices; ordering action or

1 abatement of action; adopting procedural rules; holding
 2 hearings; and any other act necessary to the performance of
 3 a quasi-judicial function.

4 {10}(11) "Quasi-legislative function" generally means
 5 making or having the power to make rules or set rates and
 6 all other acts connected with or essential to the proper
 7 exercise of a quasi-legislative function."

8 NEW SECTION. Section 2. Responsibilities of
 9 departments. Each department head is responsible for
 10 assuring an adequate level of security for all data and
 11 information technology resources within his department and
 12 shall:

13 (1) develop and annually--update MAINTAIN written
 14 internal policies and procedures to assure security of data
 15 and information technology resources. The internal policies
 16 and procedures are confidential information and exempt from
 17 public inspection, except that such information must be
 18 available to the legislative auditor in performing his
 19 postauditing duties.

20 (2) designate an information security manager to
 21 administer the department's security program for data and
 22 information technology resources;

23 {11}--conduct-and-annually-update--a--risk--analysis--to
 24 determine---security---threats---to---data--and--information
 25 technology--resources;--The--risk-analysis--information--is

1 ~~confidential--and-exempt-from-public-inspection,--except-that~~
 2 ~~such--information--must--be--available--to--the--legislative~~
 3 ~~auditor-in-performing-his-postauditing-duties.~~

4 {4}{3} implement appropriate cost-effective safeguards
 5 to reduce, eliminate, or recover from the identified risks
 6 IDENTIFIED THREATS to data and information technology
 7 resources;

8 {5}{4} ensure that ~~annual~~ internal evaluations of the
 9 security program for data and information technology
 10 resources are conducted. The results of such internal
 11 evaluations are confidential and exempt from public
 12 inspection, except that such information must be available
 13 to the legislative auditor in performing his postauditing
 14 duties.

15 {6}{5} include appropriate security requirements, as
 16 determined by the department, in the written specifications
 17 for the department's solicitation of data and information
 18 technology resources; AND

19 {7}{6} maintain an information technology plan,
 20 including a general description of the existing security
 21 program and future plans for assuring security of data and
 22 information technology resources; and.

23 {8}--certify--annually--to--the--department--of
 24 ~~administration--that--the--security--program--for--data--and~~
 25 ~~information-technology-resources-conforms-with-the-standards~~

1 ~~and---guidelines---developed---by---the---department---of~~
 2 ~~administration--A-department-that-is-unable-to-certify-its~~
 3 ~~conformance--shall-give-written-notice-to-the-department-of~~
 4 ~~administration,--stating-the-deficiencies-and-the-reasons-for~~
 5 ~~nonconformance.~~

6 NEW SECTION. Section 3. Responsibilities of
 7 department of administration. The department of
 8 administration is responsible for providing centralized
 9 management and coordination of state policies for security
 10 of data and information technology resources and shall:

11 (1) establish and maintain the minimum security
 12 standards, ~~rules, and regulations~~ AND POLICIES to implement
 13 [section 2], including the physical security of central and
 14 backup computer facilities consistent with these standards;

15 (2) establish guidelines to assist agencies in
 16 identifying electronic data processing personnel occupying
 17 positions of special trust or responsibility or sensitive
 18 locations;

19 (3) establish ~~rules--and--regulations~~ STANDARDS AND
 20 POLICIES for the exchange of data between data centers or
 21 departments by hardwired or nondedicated telecommunications
 22 to ensure that exchanges do not jeopardize data security and
 23 confidentiality;

24 (4) coordinate and provide for a training program
 25 regarding security of data and information technology

1 resources to serve governmental technical and managerial
2 needs;

3 (5) include appropriate security requirements in the
4 specifications for solicitation of state contracts for
5 procuring data and information technology resources; and

6 (6) upon request, provide technical and managerial
7 assistance relating to the security program.

8 NEW SECTION. Section 4. Responsibilities of board of
9 regents. The board of regents is responsible for assuring an
10 adequate level of security for data and information
11 technology resources, as defined in 2-15-102, within the
12 state university system. In carrying out this
13 responsibility, the board of regents shall, at a minimum,
14 address the responsibilities prescribed in [section 2].

15 NEW SECTION. Section 5. Responsibilities of supreme
16 court. The supreme court is responsible for assuring an
17 adequate level of security for data and information
18 technology resources, as defined in 2-15-102, within the
19 judicial branch. In carrying out this responsibility, the
20 supreme court shall, at a minimum:

21 (1) address the responsibilities prescribed in
22 [section 2]; and

23 (2) develop written minimum standards and guidelines
24 for the judicial branch to follow in developing its security
25 program.

1 NEW SECTION. Section 6. Codification instructions.

2 (1) Sections 2 and 3 are intended to be codified as an
3 integral part of Title 2, chapter 15, part 10, and the
4 provisions of Title 2, chapter 15, part 10, apply to
5 sections 2 and 3.

6 (2) Section 4 is intended to be codified as an
7 integral part of Title 2, chapter 15, part 15, and the
8 provisions of Title 2, chapter 15, part 15, apply to section
9 4.

10 (3) Section 5 is intended to be codified as an
11 integral part of Title 3, chapter 2, part 6, and the
12 provisions of Title 3, chapter 2, part 6, apply to section
13 5.

-End-

1 SENATE BILL NO. 279

2 INTRODUCED BY KEATING, GAGE, JACOBSON, NEUMAN,

3 SIMON, FRITZ, BRADLEY, COBB

4 BY REQUEST OF THE LEGISLATIVE AUDIT COMMITTEE

5
6 A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING FOR SECURITY
7 OF DATA AND INFORMATION TECHNOLOGY RESOURCES; ESTABLISHING
8 THE RESPONSIBILITIES OF STATE AGENCIES, THE BOARD OF
9 REGENTS, THE SUPREME COURT, AND THE DEPARTMENT OF
10 ADMINISTRATION; AND AMENDING SECTION 2-15-102, MCA."

11
12 WHEREAS, data and information collected and maintained
13 by state government are assets which require protection; and

14 WHEREAS, the increasing use of information technology
15 in state government requires a systematic risk-management
16 approach to minimize increased security threats to data and
17 information technology resources; and

18 WHEREAS, it is desirable to create a greater awareness
19 regarding the importance of security of state government
20 data and information technology resources; and

21 WHEREAS, a recent audit of mainframe computer security
22 indicated a lack of security over data processing equipment
23 and procedures.

24
25 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

1 Section 1. Section 2-15-102, MCA, is amended to read:

2 "2-15-102. Definitions. As used in this chapter, the
3 following definitions apply:

4 (1) "Executive branch" means the executive branch of
5 state government referred to in the Montana constitution,
6 Articles III and VI.

7 (2) "Agency" means an office, position, commission,
8 committee, board, department, council, division, bureau,
9 section, or any other entity or instrumentality of the
10 executive branch of state government.

11 (3) "Unit" means an internal subdivision of an agency,
12 created by law or by administrative action, including a
13 division, bureau, section, or department, and an agency
14 allocated to a department for administrative purposes only
15 by this chapter.

16 (4) "Data and information technology resources" means
17 data processing mainframe, microcomputer hardware,
18 peripherals, software, service--supplies SPECIAL FORMS,
19 personnel, facility resources, maintenance, training,
20 ELECTRONICALLY STORED DATA, or other related resources.

21 (4)(5) "Department" means a principal functional and
22 administrative entity, created by this chapter within the
23 executive branch of state government; is one of the 20
24 principal departments permitted under the constitution; and
25 includes its units.

1 †5†(6) "Department head" means a director, commission,
2 board, commissioner, or constitutional officer in charge of
3 a department created by this chapter.

4 †6†(7) "Director" means a department head specifically
5 referred to as a director in this chapter, and does not mean
6 a commission, board, commissioner, or constitutional
7 officer.

8 †7†(8) "Advisory capacity" means furnishing advice,
9 gathering information, making recommendations, and
10 performing such other activities as may be necessary to
11 comply with federal funding requirements and does not mean
12 administering a program or function or setting policy.

13 †8†(9) "Function" means a duty, power, or program,
14 exercised by or assigned to an agency, whether or not
15 specifically provided for by law.

16 †9†(10) "Quasi-judicial function" means an adjudicator,
17 function exercised by an agency, involving the exercise of
18 judgment and discretion in making determinations in
19 controversies. The term includes but is not limited to the
20 functions of interpreting, applying, and enforcing existing
21 rules and laws; granting or denying privileges, rights, or
22 benefits; issuing, suspending, or revoking licenses,
23 permits, and certificates; determining rights and interests
24 of adverse parties; evaluating and passing on facts;
25 awarding compensation; fixing prices; ordering action or

1 abatement of action; adopting procedural rules; holding
2 hearings; and any other act necessary to the performance of
3 a quasi-judicial function.

4 †10†(11) "Quasi-legislative function" generally means
5 making or having the power to make rules or set rates and
6 all other acts connected with or essential to the proper
7 exercise of a quasi-legislative function."

8 NEW SECTION. Section 2. Responsibilities of
9 departments. Each department head is responsible for
10 assuring an adequate level of security for all data and
11 information technology resources within his department and
12 shall:

13 (1) develop and ~~annually--update~~ MAINTAIN written
14 internal policies and procedures to assure security of data
15 and information technology resources. The internal policies
16 and procedures are confidential information and exempt from
17 public inspection, except that such information must be
18 available to the legislative auditor in performing his
19 postauditing duties.

20 (2) designate an information security manager to
21 administer the department's security program for data and
22 information technology resources;

23 ~~†3†--conduct-and-annually-update-a--risk--analysis--to~~
24 ~~determine---security---threats---to---data--and--information~~
25 ~~technology--resources---The--risk-analysis--information---is~~

1 ~~confidential--and-exempt-from-public-inspection, except that~~
2 ~~such--information--must--be--available--to--the--legislative~~
3 ~~auditor-in-performing-his-postauditing-duties;~~

4 {4}{3} implement appropriate cost-effective safeguards
5 to reduce, eliminate, or recover from the-identified-risks
6 IDENTIFIED THREATS to data and information technology
7 resources;

8 {5}{4} ensure that-annual internal evaluations of the
9 security program for data and information technology
10 resources are conducted. The results of such internal
11 evaluations are confidential and exempt from public
12 inspection, except that such information must be available
13 to the legislative auditor in performing his postauditing
14 duties.

15 {6}{5} include appropriate security requirements, as
16 determined by the department, in the written specifications
17 for the department's solicitation of data and information
18 technology resources; AND

19 {7}{6} maintain an information technology plan,
20 including a general description of the existing security
21 program and future plans for assuring security of data and
22 information technology resources; and.

23 {8}--certify--annually--to--the--department--of
24 ~~administration--that--the--security--program--for--data--and~~
25 ~~information-technology-resources-conforms-with-the-standards~~

1 ~~and---guidelines---developed---by---the---department---of~~
2 ~~administration--A-department-that-is-unable-to--certify--its~~
3 ~~conformance--shall--give-written-notice-to-the-department-of~~
4 ~~administration, stating the deficiencies and the reasons for~~
5 ~~nonconformance;~~

6 NEW SECTION. Section 3. Responsibilities of
7 department of administration. The department of
8 administration is responsible for providing centralized
9 management and coordination of state policies for security
10 of data and information technology resources and shall:

11 (1) establish and maintain the minimum security
12 standards, ~~rules, and regulations~~ AND POLICIES to implement
13 [section 2], including the physical security of central and
14 backup computer facilities consistent with these standards;

15 (2) establish guidelines to assist agencies in
16 identifying electronic data processing personnel occupying
17 positions of special trust or responsibility or sensitive
18 locations;

19 (3) establish ~~rules--and--regulations~~ STANDARDS AND
20 POLICIES for the exchange of data between data centers or
21 departments by hardwired or nondedicated telecommunications
22 to ensure that exchanges do not jeopardize data security and
23 confidentiality;

24 (4) coordinate and provide for a training program
25 regarding security of data and information technology

1 resources to serve governmental technical and managerial
2 needs;

3 (5) include appropriate security requirements in the
4 specifications for solicitation of state contracts for
5 procuring data and information technology resources; and

6 (6) upon request, provide technical and managerial
7 assistance relating to the security program.

8 NEW SECTION. Section 4. Responsibilities of board of
9 regents. The board of regents is responsible for assuring an
10 adequate level of security for data and information
11 technology resources, as defined in 2-15-102, within the
12 state university system. In carrying out this
13 responsibility, the board of regents shall, at a minimum,
14 address the responsibilities prescribed in [section 2].

15 NEW SECTION. Section 5. Responsibilities of supreme
16 court. The supreme court is responsible for assuring an
17 adequate level of security for data and information
18 technology resources, as defined in 2-15-102, within the
19 judicial branch. In carrying out this responsibility, the
20 supreme court shall, at a minimum:

21 (1) address the responsibilities prescribed in
22 [section 2]; and

23 (2) develop written minimum standards and guidelines
24 for the judicial branch to follow in developing its security
25 program.

1 NEW SECTION. Section 6. Codification instructions.
2 (1) Sections 2 and 3 are intended to be codified as an
3 integral part of Title 2, chapter 15, part 10, and the
4 provisions of Title 2, chapter 15, part 10, apply to
5 sections 2 and 3.

6 (2) Section 4 is intended to be codified as an
7 integral part of Title 2, chapter 15, part 15, and the
8 provisions of Title 2, chapter 15, part 15, apply to section
9 4.

10 (3) Section 5 is intended to be codified as an
11 integral part of Title 3, chapter 2, part 6, and the
12 provisions of Title 3, chapter 2, part 6, apply to section
13 5.

-End-

1 SENATE BILL NO. 279

2 INTRODUCED BY KEATING, GAGE, JACOBSON, NEUMAN,

3 SIMON, FRITZ, BRADLEY, COBB

4 BY REQUEST OF THE LEGISLATIVE AUDIT COMMITTEE

5
6 A BILL FOR AN ACT ENTITLED: "AN ACT PROVIDING FOR SECURITY
7 OF DATA AND INFORMATION TECHNOLOGY RESOURCES; ESTABLISHING
8 THE RESPONSIBILITIES OF STATE AGENCIES, THE BOARD OF
9 REGENTS, THE SUPREME COURT, AND THE DEPARTMENT OF
10 ADMINISTRATION; AND AMENDING SECTION 2-15-102, MCA."

11
12 WHEREAS, data and information collected and maintained
13 by state government are assets which require protection; and

14 WHEREAS, the increasing use of information technology
15 in state government requires a systematic risk-management
16 approach to minimize increased security threats to data and
17 information technology resources; and

18 WHEREAS, it is desirable to create a greater awareness
19 regarding the importance of security of state government
20 data and information technology resources; and

21 WHEREAS, a recent audit of mainframe computer security
22 indicated a lack of security over data processing equipment
23 and procedures.

24
25 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

1 Section 1. Section 2-15-102, MCA, is amended to read:

2 "2-15-102. Definitions. As used in this chapter, the
3 following definitions apply:

4 (1) "Executive branch" means the executive branch of
5 state government referred to in the Montana constitution,
6 Articles III and VI.

7 (2) "Agency" means an office, position, commission,
8 committee, board, department, council, division, bureau,
9 section, or any other entity or instrumentality of the
10 executive branch of state government.

11 (3) "Unit" means an internal subdivision of an agency,
12 created by law or by administrative action, including a
13 division, bureau, section, or department, and an agency
14 allocated to a department for administrative purposes only
15 by this chapter.

16 (4) "Data and information technology resources" means
17 data processing mainframe, microcomputer hardware,
18 peripherals, software, ~~service--supplies~~ SPECIAL FORMS,
19 personnel, facility resources, maintenance, training,
20 ELECTRONICALLY STORED DATA, or other related resources.

21 (4)(5) "Department" means a principal functional and
22 administrative entity, created by this chapter within the
23 executive branch of state government; is one of the 20
24 principal departments permitted under the constitution; and
25 includes its units.

1 †5)†6) "Department head" means a director, commission,
2 board, commissioner, or constitutional officer in charge of
3 a department created by this chapter.

4 †6)†7) "Director" means a department head specifically
5 referred to as a director in this chapter, and does not mean
6 a commission, board, commissioner, or constitutional
7 officer.

8 †7)†8) "Advisory capacity" means furnishing advice,
9 gathering information, making recommendations, and
10 performing such other activities as may be necessary to
11 comply with federal funding requirements and does not mean
12 administering a program or function or setting policy.

13 †8)†9) "Function" means a duty, power, or program,
14 exercised by or assigned to an agency, whether or not
15 specifically provided for by law.

16 †9)†10) "Quasi-judicial function" means an adjudicatory
17 function exercised by an agency, involving the exercise of
18 judgment and discretion in making determinations in
19 controversies. The term includes but is not limited to the
20 functions of interpreting, applying, and enforcing existing
21 rules and laws; granting or denying privileges, rights, or
22 benefits; issuing, suspending, or revoking licenses,
23 permits, and certificates; determining rights and interests
24 of adverse parties; evaluating and passing on facts;
25 awarding compensation; fixing prices; ordering action or

1 abatement of action; adopting procedural rules; holding
2 hearings; and any other act necessary to the performance of
3 a quasi-judicial function.

4 †10)†11) "Quasi-legislative function" generally means
5 making or having the power to make rules or set rates and
6 all other acts connected with or essential to the proper
7 exercise of a quasi-legislative function."

8 NEW SECTION. Section 2. Responsibilities of
9 departments. Each department head is responsible for
10 assuring an adequate level of security for all data and
11 information technology resources within his department and
12 shall:

13 (1) develop and ~~annually--update~~ MAINTAIN written
14 internal policies and procedures to assure security of data
15 and information technology resources. The internal policies
16 and procedures are confidential information and exempt from
17 public inspection, except that such information must be
18 available to the legislative auditor in performing his
19 postauditing duties.

20 (2) designate an information security manager to
21 administer the department's security program for data and
22 information technology resources;

23 ~~†3)--conduct-and-annually-update--a--risk--analysis--to~~
24 ~~determine---security---threats---to---data--and--information~~
25 ~~technology--resources;--The--risk-analysis--information---is~~

1 ~~confidential--and-exempt-from-public-inspection, except that~~
 2 ~~such--information--must--be--available--to--the--legislative~~
 3 ~~auditor-in-performing-his-postauditing-duties;~~

4 ~~(4)(3)~~ implement appropriate cost-effective safeguards
 5 to reduce, eliminate, or recover from ~~the-identified-risks~~
 6 IDENTIFIED THREATS to data and information technology
 7 resources;

8 ~~(5)(4)~~ ensure ~~that-annual~~ internal evaluations of the
 9 security program for data and information technology
 10 resources are conducted. The results of such internal
 11 evaluations are confidential and exempt from public
 12 inspection, except that such information must be available
 13 to the legislative auditor in performing his postauditing
 14 duties.

15 ~~(6)(5)~~ include appropriate security requirements, as
 16 determined by the department, in the written specifications
 17 for the department's solicitation of data and information
 18 technology resources; AND

19 ~~(7)(6)~~ maintain an information technology plan,
 20 including a general description of the existing security
 21 program and future plans for assuring security of data and
 22 information technology resources; ~~and.~~

23 ~~(8)--certify--annually--to--the--department--of~~
 24 ~~administration--that--the--security--program--for--data--and~~
 25 ~~information-technology-resources-conforms-with-the-standards~~

1 ~~and---guidelines---developed---by---the---department---of~~
 2 ~~administration;--A-department-that-is-unable-to--certify--its~~
 3 ~~conformance--shall--give-written-notice-to-the-department-of~~
 4 ~~administration,--stating-the-deficiencies-and-the-reasons-for~~
 5 ~~nonconformance;~~

6 NEW SECTION. Section 3. Responsibilities of
 7 department of administration. The department of
 8 administration is responsible for providing centralized
 9 management and coordination of state policies for security
 10 of data and information technology resources and shall:

11 (1) establish and maintain the minimum security
 12 standards; ~~rules,--and--regulations~~ AND POLICIES to implement
 13 [section 2], including the physical security of central and
 14 backup computer facilities consistent with these standards;

15 (2) establish guidelines to assist agencies in
 16 identifying electronic data processing personnel occupying
 17 positions of special trust or responsibility or sensitive
 18 locations;

19 (3) establish ~~rules--and--regulations~~ STANDARDS AND
 20 POLICIES for the exchange of data between data centers or
 21 departments by hardwired or nondedicated telecommunications
 22 to ensure that exchanges do not jeopardize data security and
 23 confidentiality;

24 (4) coordinate and provide for a training program
 25 regarding security of data and information technology

resources to serve governmental technical and managerial needs;

(5) include appropriate security requirements in the specifications for solicitation of state contracts for procuring data and information technology resources; and

(6) upon request, provide technical and managerial assistance relating to the security program.

NEW SECTION. Section 4. Responsibilities of board of regents. The board of regents is responsible for assuring an adequate level of security for data and information technology resources, as defined in 2-15-102, within the state university system. In carrying out this responsibility, the board of regents shall, at a minimum, address the responsibilities prescribed in [section 2].

NEW SECTION. Section 5. Responsibilities of supreme court. The supreme court is responsible for assuring an adequate level of security for data and information technology resources, as defined in 2-15-102, within the judicial branch. In carrying out this responsibility, the supreme court shall, at a minimum:

(1) address the responsibilities prescribed in [section 2]; and

(2) develop written minimum standards and guidelines for the judicial branch to follow in developing its security program.

NEW SECTION. Section 6. Codification instructions.
~~(1) SECTION 2 IS INTENDED TO BE CODIFIED AS AN INTEGRAL PART OF TITLE 2, CHAPTER 15, PART 1, AND THE PROVISIONS OF TITLE 2, CHAPTER 15, PART 1, APPLY TO SECTION 2.~~

~~††(2) Sections-2-and SECTION 3 are IS intended to be codified as an integral part of Title 2, chapter †5 17, part †0 5, and the provisions of Title 2, chapter †5 17, part †0 5, apply to sections-2-and SECTION 3.~~

~~†2†(3) Section 4 is intended to be codified as an integral part of Title 2, chapter 15, part 15, and the provisions of Title 2, chapter 15, part 15, apply to section 4.~~

~~†3†(4) Section 5 is intended to be codified as an integral part of Title 3, chapter 2, part 6, and the provisions of Title 3, chapter 2, part 6, apply to section 5.~~

-End-