NOTE: This bill has been prepared for the signature of the appropriate legislative officers and the Governor. To determine whether the Governor has signed the bill or taken other action on it, please consult the legislative status sheet, the legislative history, or the Session Laws.

An Act

HOUSE BILL 06-1157

BY REPRESENTATIVE(S) Coleman, Buescher, Garcia, Marshall, Romanoff, Stengel, White, Frangas, Hall, McFadyen, Paccione, Penry, Rose, Stafford, Berens, and Green;
also SENATOR(S) May R., Williams, Entz, Fitz-Gerald, Jones, Owen, Taylor, and Teck.

CONCERNING THE SECURITY OF COMMUNICATION AND INFORMATION RESOURCES IN PUBLIC AGENCIES, AND MAKING AN APPROPRIATION IN CONNECTION THEREWITH.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. Article 37.5 of title 24, Colorado Revised Statutes, is amended BY THE ADDITION OF A NEW PART to read:

PART 4
INFORMATION SECURITY

24-37.5-401. Legislative declaration. (1) THE GENERAL ASSEMBLY HEREBY FINDS, DETERMINES, AND DECLARES THAT:

(a) COMMUNICATION AND INFORMATION RESOURCES IN THE VARIOUS PUBLIC AGENCIES OF THE STATE ARE STRATEGIC AND VITAL ASSETS

Capital letters indicate new material added to existing statutes; dashes through words indicate deletions from existing statutes and such material not part of act.

BELONGING TO THE PEOPLE OF COLORADO. COORDINATED EFFORTS AND A SENSE OF URGENCY ARE NECESSARY TO PROTECT THESE ASSETS AGAINST UNAUTHORIZED ACCESS, DISCLOSURE, USE, AND MODIFICATION OR DESTRUCTION, WHETHER ACCIDENTAL OR DELIBERATE, AS WELL AS TO ASSURE THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF INFORMATION.

(b) STATE GOVERNMENT HAS A DUTY TO COLORADO'S CITIZENS TO ENSURE THAT THE INFORMATION THE CITIZENS HAVE ENTRUSTED TO PUBLIC AGENCIES IS SAFE, SECURE, AND PROTECTED FROM UNAUTHORIZED ACCESS, UNAUTHORIZED USE, OR DESTRUCTION.

(c) SECURING THE STATE'S COMMUNICATION AND INFORMATION RESOURCES IS A STATEWIDE IMPERATIVE REQUIRING A COORDINATED AND SHARED EFFORT FROM ALL DEPARTMENTS, AGENCIES, AND POLITICAL SUBDIVISIONS OF THE STATE AND A LONG TERM COMMITMENT TO STATE FUNDING THAT ENSURES THE SUCCESS OF SUCH EFFORTS.

(d) RISKS TO COMMUNICATION AND INFORMATION RESOURCES MUST BE MANAGED, AND THE INTEGRITY OF DATA AND THE SOURCE, DESTINATION, AND PROCESSES APPLIED TO DATA MUST BE ASSURED.

(e) INFORMATION SECURITY STANDARDS, POLICIES, AND GUIDELINES MUST BE PROMULGATED AND IMPLEMENTED THROUGHOUT PUBLIC AGENCIES TO ENSURE THE DEVELOPMENT AND MAINTENANCE OF MINIMUM INFORMATION SECURITY CONTROLS TO PROTECT COMMUNICATION AND INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THOSE AGENCIES.

(f) THE EXTENSIVE INFORMATION SECURITY EXPERTISE IN COLORADO'S PRIVATE SECTOR SHOULD BE UTILIZED FOR THE LONG-TERM BENEFIT OF COLORADO'S CITIZENS AND PUBLIC AGENCIES.

24-37.5-402. Definitions. AS USED IN THIS PART 4, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(1) "AVAILABILITY" MEANS THE TIMELY AND RELIABLE ACCESS TO AND USE OF INFORMATION CREATED, GENERATED, COLLECTED, OR MAINTAINED BY A PUBLIC AGENCY.

(2) "COMMUNICATION AND INFORMATION RESOURCES" SHALL HAVE THE SAME MEANING AS PROVIDED IN SECTION 24-37.5-102 (1).

(3) "CONFIDENTIALITY" MEANS THE PRESERVATION OF AUTHORIZED RESTRICTIONS ON INFORMATION ACCESS AND DISCLOSURE, INCLUDING THE MEANS FOR PROTECTING PERSONAL PRIVACY AND PROPRIETARY INFORMATION.

(4) "DEPARTMENT OF HIGHER EDUCATION" MEANS THE COLORADO COMMISSION ON HIGHER EDUCATION, COLLEGEINVEST, THE COLORADO STUDENT LOAN PROGRAM, THE COLORADO COLLEGE ACCESS NETWORK, THE PRIVATE OCCUPATIONAL SCHOOL DIVISION, THE STATE HISTORICAL SOCIETY, AND THE STATE COUNCIL ON THE ARTS.

(5) "INFORMATION SECURITY" MEANS THE PROTECTION OF COMMUNICATION AND INFORMATION RESOURCES FROM UNAUTHORIZED ACCESS, USE, DISCLOSURE, DISRUPTION, MODIFICATION, OR DESTRUCTION IN ORDER TO:

(a) PREVENT IMPROPER INFORMATION MODIFICATION OR DESTRUCTION;

(b) PRESERVE AUTHORIZED RESTRICTIONS ON INFORMATION ACCESS AND DISCLOSURE;

(c) ENSURE TIMELY AND RELIABLE ACCESS TO AND USE OF INFORMATION; AND

(d) MAINTAIN THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF INFORMATION.

(6) "INFORMATION SECURITY PLAN" MEANS THE PLAN DEVELOPED BY A PUBLIC AGENCY PURSUANT TO SECTION 24-37.5-404.

(7) "INSTITUTION OF HIGHER EDUCATION" MEANS A STATE-SUPPORTED INSTITUTION OF HIGHER EDUCATION.

(8) "INTEGRITY" MEANS THE PREVENTION OF IMPROPER INFORMATION MODIFICATION OR DESTRUCTION AND ENSURING INFORMATION NONREPUDIATION AND AUTHENTICITY.

(9) "PUBLIC AGENCY" MEANS EVERY STATE OFFICE, WHETHER LEGISLATIVE, EXECUTIVE, OR JUDICIAL, AND ALL OF ITS RESPECTIVE OFFICES, DEPARTMENTS, DIVISIONS, COMMISSIONS, BOARDS, BUREAUS, AND INSTITUTIONS. "PUBLIC AGENCY" DOES NOT INCLUDE INSTITUTIONS OF HIGHER EDUCATION OR THE DEPARTMENT OF HIGHER EDUCATION.

(10) "SECURITY INCIDENT" MEANS AN ACCIDENTAL OR DELIBERATE EVENT THAT RESULTS IN OR CONSTITUTES AN IMMINENT THREAT OF THE UNAUTHORIZED ACCESS, LOSS, DISCLOSURE, MODIFICATION, DISRUPTION, OR DESTRUCTION OF COMMUNICATION AND INFORMATION RESOURCES.

24-37.5-403. Chief information security officer - duties and responsibilities. (1) THE GOVERNOR SHALL APPOINT A CHIEF INFORMATION SECURITY OFFICER WHO SHALL SERVE AT THE PLEASURE OF THE GOVERNOR. THE OFFICER SHALL EXHIBIT A BACKGROUND AND EXPERTISE IN SECURITY AND RISK MANAGEMENT FOR COMMUNICATIONS AND INFORMATION RESOURCES. IN THE EVENT THE OFFICER IS UNAVAILABLE TO PERFORM THE DUTIES AND RESPONSIBILITIES UNDER THIS PART 4, ALL POWERS AND AUTHORITY GRANTED TO THE OFFICER MAY BE EXERCISED BY THE CHIEF TECHNOLOGY OFFICER IN THE OFFICE OF INNOVATION AND TECHNOLOGY.

(2) THE CHIEF INFORMATION SECURITY OFFICER SHALL:

(a) DEVELOP AND UPDATE INFORMATION SECURITY POLICIES, STANDARDS, AND GUIDELINES FOR PUBLIC AGENCIES;

(b) PROMULGATE RULES PURSUANT TO ARTICLE 4 OF THIS TITLE CONTAINING INFORMATION SECURITY POLICIES, STANDARDS, AND GUIDELINES FOR SUCH AGENCIES ON OR BEFORE DECEMBER 31, 2006;

(c) ENSURE THE INCORPORATION OF AND COMPLIANCE WITH INFORMATION SECURITY POLICIES, STANDARDS, AND GUIDELINES IN THE INFORMATION SECURITY PLANS DEVELOPED BY PUBLIC AGENCIES PURSUANT TO SECTION 24-37.5-404;

(d) DIRECT INFORMATION SECURITY AUDITS AND ASSESSMENTS IN PUBLIC AGENCIES IN ORDER TO ENSURE PROGRAM COMPLIANCE AND ADJUSTMENTS;

(e) ESTABLISH AND DIRECT A RISK MANAGEMENT PROCESS TO

IDENTIFY INFORMATION SECURITY RISKS IN PUBLIC AGENCIES AND DEPLOY RISK MITIGATION STRATEGIES, PROCESSES, AND PROCEDURES;

(f) APPROVE OR DISAPPROVE AND REVIEW ANNUALLY THE INFORMATION SECURITY PLANS OF PUBLIC AGENCIES;

(g) CONDUCT INFORMATION SECURITY AWARENESS AND TRAINING PROGRAMS;

(h) IN COORDINATION AND CONSULTATION WITH THE OFFICE OF STATE PLANNING AND BUDGETING AND THE CHIEF TECHNOLOGY OFFICER, REVIEW PUBLIC AGENCY BUDGET REQUESTS RELATED TO INFORMATION SECURITY SYSTEMS AND APPROVE SUCH BUDGET REQUESTS FOR STATE AGENCIES OTHER THAN THE LEGISLATIVE DEPARTMENT; AND

(i) COORDINATE WITH THE COLORADO COMMISSION ON HIGHER EDUCATION FOR PURPOSES OF REVIEWING AND COMMENTING ON INFORMATION SECURITY PLANS ADOPTED BY INSTITUTIONS OF HIGHER EDUCATION THAT ARE SUBMITTED PURSUANT TO SECTION 24-37.5-404.5 (3).

(3) FOR THE STATE FISCAL YEAR COMMENCING ON JULY 1, 2006, THE COST OF THE SERVICES PROVIDED BY THE CHIEF INFORMATION SECURITY OFFICER TO PUBLIC AGENCIES IN ADMINISTERING THIS PART 4 SHALL BE PAID FROM FEDERAL FUNDS RECEIVED BY THE STATE FOR SUCH PURPOSES. IT IS THE INTENT OF THE GENERAL ASSEMBLY THAT THE COST OF THE SERVICES PROVIDED BY THE CHIEF INFORMATION SECURITY OFFICER TO A PUBLIC AGENCY BE ADEQUATELY FUNDED IN FISCAL YEARS COMMENCING ON AND AFTER JULY 1, 2007, THROUGH AN APPROPRIATION TO THE PUBLIC AGENCY TO PAY FOR SUCH SERVICES.

24-37.5-404. Public agencies - information security plans. (1) ON OR BEFORE JULY 1, 2007, EACH PUBLIC AGENCY SHALL DEVELOP AN INFORMATION SECURITY PLAN UTILIZING THE INFORMATION SECURITY POLICIES, STANDARDS, AND GUIDELINES DEVELOPED BY THE CHIEF INFORMATION SECURITY OFFICER. THE INFORMATION SECURITY PLAN SHALL PROVIDE INFORMATION SECURITY FOR THE COMMUNICATION AND INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE PUBLIC AGENCY.

(2) THE INFORMATION SECURITY PLAN SHALL INCLUDE:

(a) PERIODIC ASSESSMENTS OF THE RISK AND MAGNITUDE OF THE HARM THAT COULD RESULT FROM A SECURITY INCIDENT;

(b) A PROCESS FOR PROVIDING ADEQUATE INFORMATION SECURITY FOR THE COMMUNICATION AND INFORMATION RESOURCES OF THE PUBLIC AGENCY;

(c) REGULARIZED SECURITY AWARENESS TRAINING TO INFORM THE EMPLOYEES AND USERS OF THE PUBLIC AGENCY'S COMMUNICATION AND INFORMATION RESOURCES ABOUT INFORMATION SECURITY RISKS AND THE RESPONSIBILITY OF EMPLOYEES AND USERS TO COMPLY WITH AGENCY POLICIES, STANDARDS, AND PROCEDURES DESIGNED TO REDUCE THOSE RISKS;

(d) PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF INFORMATION SECURITY FOR THE PUBLIC AGENCY, WHICH SHALL BE PERFORMED NOT LESS THAN ANNUALLY;

(e) A PROCESS FOR DETECTING, REPORTING, AND RESPONDING TO SECURITY INCIDENTS CONSISTENT WITH THE INFORMATION SECURITY STANDARDS, POLICIES, AND GUIDELINES ISSUED BY THE CHIEF INFORMATION SECURITY OFFICER; AND

(f) PLANS AND PROCEDURES TO ENSURE THE CONTINUITY OF OPERATIONS FOR INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE PUBLIC AGENCY IN THE EVENT OF A SECURITY INCIDENT.

(3) ON OR BEFORE JULY 15, 2007, EACH PUBLIC AGENCY SHALL SUBMIT THE INFORMATION SECURITY PLAN DEVELOPED PURSUANT TO THIS SECTION TO THE CHIEF INFORMATION SECURITY OFFICER FOR APPROVAL.

(4) IN THE EVENT THAT A PUBLIC AGENCY FAILS TO SUBMIT TO THE CHIEF INFORMATION SECURITY OFFICER AN INFORMATION SECURITY PLAN ON OR BEFORE JULY 15, 2007, OR SUCH PLAN IS DISAPPROVED BY THE CHIEF INFORMATION SECURITY OFFICER, THE OFFICER SHALL NOTIFY THE GOVERNOR AND THE HEAD AND CHIEF INFORMATION OFFICER OF THE PUBLIC AGENCY OF NONCOMPLIANCE WITH THIS SECTION. IF NO PLAN HAS BEEN APPROVED BY SEPTEMBER 15, 2007, THE OFFICER SHALL BE AUTHORIZED TO TEMPORARILY DISCONTINUE OR SUSPEND THE OPERATION OF A PUBLIC AGENCY'S COMMUNICATION AND INFORMATION RESOURCES UNTIL SUCH

PLAN HAS BEEN SUBMITTED TO OR IS APPROVED BY THE OFFICER.

(5) AN INFORMATION SECURITY PLAN MAY PROVIDE FOR A PHASE-IN PERIOD NOT TO EXCEED THREE YEARS. AN IMPLEMENTATION SCHEDULE FOR THE PHASE-IN PERIOD SHALL BE INCLUDED IN SUCH A PLAN. ANY PHASE-IN PERIOD PURSUANT TO THIS SUBSECTION (5) SHALL BE COMPLETED BY JULY 1, 2009.

(6) ON OR BEFORE JULY 1, 2008, AND ON OR BEFORE JULY 1 OF EACH SUBSEQUENT YEAR, THE EXECUTIVE DIRECTOR OR HEAD OF EACH PUBLIC AGENCY SHALL REPORT TO THE CHIEF INFORMATION SECURITY OFFICER ON THE DEVELOPMENT, IMPLEMENTATION, AND, IF APPLICABLE, COMPLIANCE WITH THE PHASE-IN SCHEDULE OF THE PUBLIC AGENCY'S INFORMATION SECURITY PLAN.

24-37.5-404.5. Institutions of higher education - information security plans. (1) ON OR BEFORE JULY 1, 2007, EACH INSTITUTION OF HIGHER EDUCATION, IN COORDINATION WITH THE COLORADO COMMISSION ON HIGHER EDUCATION, SHALL DEVELOP AN INFORMATION SECURITY PLAN. THE INFORMATION SECURITY PLAN SHALL PROVIDE INFORMATION SECURITY FOR THE COMMUNICATION AND INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE INSTITUTION OF HIGHER EDUCATION.

(2) THE INFORMATION SECURITY PLAN SHALL INCLUDE:

(a) PERIODIC ASSESSMENTS OF THE RISK AND MAGNITUDE OF THE HARM THAT COULD RESULT FROM A SECURITY INCIDENT;

(b) A PROCESS FOR PROVIDING ADEQUATE INFORMATION SECURITY FOR THE COMMUNICATION AND INFORMATION RESOURCES OF THE INSTITUTION OF HIGHER EDUCATION;

(c) INFORMATION SECURITY AWARENESS TRAINING FOR EMPLOYEES OF THE INSTITUTION OF HIGHER EDUCATION;

(d) PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF INFORMATION SECURITY FOR THE INSTITUTION OF HIGHER EDUCATION, WHICH SHALL BE PERFORMED NOT LESS THAN ANNUALLY;

(e) A PROCESS FOR DETECTING, REPORTING, AND RESPONDING TO

SECURITY INCIDENTS CONSISTENT WITH THE INFORMATION SECURITY POLICY OF THE INSTITUTION OF HIGHER EDUCATION. THE INSTITUTIONS OF HIGHER EDUCATION, THE COLORADO COMMISSION ON HIGHER EDUCATION, AND THE CHIEF INFORMATION SECURITY OFFICER SHALL ESTABLISH THE TERMS AND CONDITIONS BY WHICH THE INSTITUTIONS OF HIGHER EDUCATION AND THE DEPARTMENT OF HIGHER EDUCATION SHALL REPORT INFORMATION SECURITY INCIDENTS TO THE CHIEF INFORMATION SECURITY OFFICER.

(f) PLANS AND PROCEDURES TO ENSURE THE CONTINUITY OF OPERATIONS FOR INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE INSTITUTION OF HIGHER EDUCATION IN THE EVENT OF A SECURITY INCIDENT.

(3) ON OR BEFORE JULY 15, 2007, EACH INSTITUTION OF HIGHER EDUCATION SHALL SUBMIT THE INFORMATION SECURITY PLAN DEVELOPED PURSUANT TO THIS SECTION TO THE COLORADO COMMISSION ON HIGHER EDUCATION FOR REVIEW AND COMMENT. THE COMMISSION SHALL SUBMIT SUCH PLANS TO THE CHIEF INFORMATION SECURITY OFFICER.

(4) NOTHING IN THIS SECTION SHALL BE CONSTRUED TO REQUIRE ANY INSTITUTION OF HIGHER EDUCATION OR THE DEPARTMENT OF HIGHER EDUCATION TO ADOPT POLICIES OR STANDARDS THAT CONFLICT WITH FEDERAL LAW, RULES, OR REGULATIONS OR WITH CONTRACTUAL ARRANGEMENTS GOVERNED BY FEDERAL LAWS, RULES, OR REGULATIONS.

(5) AN INFORMATION SECURITY PLAN MAY PROVIDE FOR A PHASE-IN PERIOD NOT TO EXCEED THREE YEARS. AN IMPLEMENTATION SCHEDULE FOR THE PHASE-IN PERIOD SHALL BE INCLUDED IN SUCH A PLAN. ANY PHASE-IN PERIOD PURSUANT TO THIS SUBSECTION (5) SHALL BE COMPLETED BY JULY 1, 2009.

(6) ON OR BEFORE JULY 1, 2008, AND ON OR BEFORE JULY 1 OF EACH SUBSEQUENT YEAR, THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF HIGHER EDUCATION SHALL REPORT TO THE CHIEF INFORMATION SECURITY OFFICER ON THE DEVELOPMENT, IMPLEMENTATION, AND, IF APPLICABLE, COMPLIANCE WITH THE PHASE-IN SCHEDULE OF THE INFORMATION SECURITY PLAN FOR EACH INSTITUTION OF HIGHER EDUCATION.

(7) THE COLORADO COMMISSION ON HIGHER EDUCATION SHALL REQUIRE THE INSTITUTIONS OF HIGHER EDUCATION TO PROVIDE

REGULARIZED SECURITY AWARENESS TRAINING TO INFORM THE EMPLOYEES, ADMINISTRATORS, AND USERS IN THOSE INSTITUTIONS ABOUT THE INFORMATION SECURITY RISKS AND THE RESPONSIBILITY OF EMPLOYEES, ADMINISTRATORS, AND USERS TO COMPLY WITH THE INSTITUTION'S INFORMATION SECURITY PLAN AND THE POLICIES, STANDARDS, AND PROCEDURES DESIGNED TO REDUCE THOSE RISKS.

24-37.5-405. Security incidents - authority of chief information security officer. (1) A SECURITY INCIDENT IN A PUBLIC AGENCY SHALL BE REPORTED TO THE CHIEF INFORMATION SECURITY OFFICER IN ACCORDANCE WITH STATE INCIDENT REPORTING POLICIES, STANDARDS, AND GUIDELINES.

(2) THE CHIEF INFORMATION SECURITY OFFICER SHALL BE AUTHORIZED TO TEMPORARILY DISCONTINUE OR SUSPEND THE OPERATION OF A PUBLIC AGENCY'S COMMUNICATION AND INFORMATION RESOURCES IN ORDER TO ISOLATE THE SOURCE OF A SECURITY INCIDENT. THE OFFICER SHALL GIVE NOTICE TO THE GOVERNOR, OR THE LIEUTENANT GOVERNOR IN THE EVENT THE GOVERNOR IS NOT AVAILABLE, AND THE HEAD AND CHIEF INFORMATION OFFICER OF THE PUBLIC AGENCY CONCURRENT WITH SUCH DISCONTINUATION OR SUSPENSION OF OPERATIONS. THE OFFICER SHALL ENSURE, TO THE EXTENT POSSIBLE, THE CONTINUITY OF OPERATIONS FOR THE COMMUNICATION AND INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE PUBLIC AGENCY.

(3) THE CHIEF INFORMATION SECURITY OFFICER MAY ENTER INTO CONTRACTS WITH A PRIVATE PERSON OR ENTITY TO ASSIST WITH RESOLVING A SECURITY INCIDENT IN A PUBLIC AGENCY. THE OFFICER SHALL ESTABLISH AN APPROVED LIST OF CERTIFIED PRIVATE PERSONS AND ENTITIES THAT MAY PROVIDE CONTRACT SERVICES IN THE EVENT OF A SECURITY INCIDENT. THE OFFICER SHALL ESTABLISH CRITERIA FOR THE PLACEMENT OF PRIVATE PERSONS AND ENTITIES ON THE LIST AND SHALL SELECT SUCH PERSONS AND ENTITIES FOR PLACEMENT ON THE LIST UTILIZING A REQUEST FOR PROPOSALS CONTAINING SUCH CRITERIA.

(4) PUBLIC AGENCIES SHALL COMPLY AND COOPERATE WITH A DIRECTIVE OF THE CHIEF INFORMATION SECURITY OFFICER PURSUANT TO SUBSECTION (2) OF THIS SECTION TO TEMPORARILY DISCONTINUE OR SUSPEND THE OPERATION OF A PUBLIC AGENCY'S COMMUNICATION AND INFORMATION RESOURCES.

24-37.5-406. Reporting. THE CHIEF INFORMATION SECURITY OFFICER SHALL REPORT TO THE GOVERNOR AND THE COMMISSION ON INFORMATION MANAGEMENT ON A QUARTERLY BASIS CONCERNING THE IMPLEMENTATION OF THE PROVISIONS OF THIS PART 4.

SECTION 2. 24-72-202 (6) (b), Colorado Revised Statutes, is amended BY THE ADDITION OF THE FOLLOWING NEW SUBPARAGRAPHS to read:

24-72-202. Definitions. As used in this part 2, unless the context otherwise requires:

(6) (b) "Public records" does not include:

(X) THE INFORMATION SECURITY PLAN OF A PUBLIC AGENCY DEVELOPED PURSUANT TO SECTION 24-37.5-404;

(XI) INFORMATION SECURITY INCIDENT REPORTS PREPARED PURSUANT TO SECTION 24-37.5-404 (2) (e); OR

(XII) INFORMATION SECURITY AUDIT AND ASSESSMENT REPORTS PREPARED PURSUANT TO SECTION 24-37.5-403 (2) (d).

SECTION 3. Appropriation. The general assembly anticipates that, for the fiscal year beginning July 1, 2006, the office of the governor will receive the sum of four million two hundred thousand dollars ($4,200,000) in federal funds and 1.0 FTE, for the implementation of this act. Although these funds are not appropriated in this act, they are noted for the purpose of indicating the assumptions used relative to these funds.

SECTION 4. Safety clause. The general assembly hereby finds,

determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

Andrew Romanoff SPEAKER OF THE HOUSE OF REPRESENTATIVES	Joan Fitz-Gerald PRESIDENT OF THE SENATE
Marilyn Eddins CHIEF CLERK OF THE HOUSE OF REPRESENTATIVES	Karen Goldman SECRETARY OF THE SENATE

APPROVED_____

Bill Owens
GOVERNOR OF THE STATE OF COLORADO