CHAPTER 109

GENERAL ASSEMBLY

SENATE BILL 11-082

BY SENATOR(S) King S., Carroll, Renfroe, Tochtrop, Foster, Giron, Guzman, Heath, Kopp, Newell, Nicholson, Schwartz, Steadman, White;
also REPRESENTATIVE(S) Acree, Gardner D., Kerr J., Miklosi, Conti, Labuda, Pace, Stephens, Summers, Wilson.

AN ACT

CONCERNING THE AUTHORITY OF THE STATE AUDITOR TO CONDUCT AUDITS OF SECURITY SYSTEMS USED FOR INFORMATION TECHNOLOGY OPERATED BY THE STATE.

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

SECTION 1. 2-3-103, Colorado Revised Statutes, is amended BY THE ADDITION OF THE FOLLOWING NEW SUBSECTIONS to read:

2-3-103. Duties of state auditor - definitions. (1.5) (a) IN ADDITION TO ANY OTHER DUTIES GRANTED BY LAW, THE STATE AUDITOR MAY ASSESS, CONFIRM, AND REPORT ON THE SECURITY PRACTICES OF ALL OF THE INFORMATION TECHNOLOGY SYSTEMS MAINTAINED OR ADMINISTERED BY ALL DEPARTMENTS, INSTITUTIONS, AND AGENCIES OF STATE GOVERNMENT, INCLUDING EDUCATIONAL INSTITUTIONS AND THE JUDICIAL AND LEGISLATIVE BRANCHES. THE AUDITOR MAY PERFORM SIMILAR OR RELATED DUTIES WITH RESPECT TO POLITICAL SUBDIVISIONS OF THE STATE WHERE THE AUDITOR HAS BEEN GRANTED AUTHORITY TO PERFORM FINANCIAL OR PERFORMANCE AUDITS WITH RESPECT TO SUCH POLITICAL SUBDIVISIONS. IN ORDER TO PERFORM SUCH DUTIES, THE STATE AUDITOR MAY CONDUCT PENETRATION OR SIMILAR TESTING OF COMPUTER NETWORKS OR INFORMATION SYSTEMS OF THE STATE OR A POLITICAL SUBDIVISION, AS APPLICABLE, ASSESS NETWORK OR INFORMATION SYSTEM VULNERABILITY, OR CONDUCT SIMILAR OR RELATED PROCEDURES TO PROMOTE BEST PRACTICES WITH RESPECT TO THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF INFORMATION SYSTEMS TECHNOLOGY AS THE AUDITOR DEEMS NECESSARY IN HIS OR HER DISCRETION. IN CONDUCTING SUCH TESTING, THE STATE AUDITOR MAY CONTRACT WITH AUDITORS OR INFORMATION TECHNOLOGY SECURITY SPECIALISTS, OR BOTH, THAT POSSESS THE NECESSARY SPECIALIZED KNOWLEDGE AND EXPERIENCE TO PERFORM THE REQUIRED WORK. THE AUTHORITY OF THE STATE AUDITOR PURSUANT TO THE REQUIREMENTS OF THIS SUBSECTION (1.5) SHALL BE

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

COEXTENSIVE WITH THE AUDITOR'S AUTHORITY UNDER THIS PART 1.

(b) ANY TESTING OR ASSESSMENT OF SECURITY PRACTICES AND PROCEDURES CONCERNING INFORMATION TECHNOLOGY IN ACCORDANCE WITH PARAGRAPH (a) OF THIS SUBSECTION (1.5) SHALL BE CONDUCTED OR CAUSED TO BE CONDUCTED BY THE STATE AUDITOR:

(I) AFTER CONSULTATION AND IN COORDINATION WITH, BUT NOT REQUIRING THE APPROVAL OF, THE CHIEF INFORMATION OFFICER APPOINTED PURSUANT TO SECTION 24-37.5-103, C.R.S., OR ANY PERSON PERFORMING COMPARABLE DUTIES FOR EITHER A STATE AGENCY THAT IS NOT UNDER THE JURISDICTION OF THE OFFICE OF INFORMATION TECHNOLOGY CREATED IN SECTION 24-37.5-103, C.R.S., OR A POLITICAL SUBDIVISION OF THE STATE;

(II) IN ACCORDANCE WITH INDUSTRY STANDARDS PRESCRIBED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY OR ANY SUCCESSOR AGENCY; AND

(III) AFTER THE STATE AUDITOR AND ANY OTHER PERSON WITH WHOM THE STATE AUDITOR IS REQUIRED TO CONSULT IN ACCORDANCE WITH THE REQUIREMENTS OF SUBPARAGRAPH (I) OF THIS PARAGRAPH (b) HAVE AGREED IN WRITING TO RULES GOVERNING THE MANNER IN WHICH THE TESTING OR ASSESSMENT IS TO BE CONDUCTED, INCLUDING A MITIGATION PLAN FOR HANDLING SIGNIFICANT SYSTEM OUTAGES OR DISRUPTIONS IN THE EVENT THEY OCCUR.

(10) AS USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(a) "INFORMATION TECHNOLOGY" SHALL HAVE THE SAME MEANING AS SPECIFIED IN SECTION 24-37.5-102 (2), C.R.S.

SECTION 2. 2-3-107 (2) (b), Colorado Revised Statutes, is amended to read:

2-3-107. Authority to subpoena witnesses - access to records. (2) (b) Nothing in this subsection (2) shall be construed as authorizing or permitting the publication of information prohibited by law. Notwithstanding the approval of the committee to release work papers of the office of the state auditor pursuant to section 2-3-103 (3), no information required to be kept confidential pursuant to any other law shall be released in connection with an audit. THE RESULTS OF ANY AUDIT OR EVALUATION OF INFORMATION TECHNOLOGY SYSTEMS UNDERTAKEN PURSUANT TO SECTION 2-3-103 (1.5) THAT ARE PRECLUDED FROM DISCLOSURE UNDER SECTION 24-6-402 (3) (a) (IV), C.R.S., SHALL NOT BE RELEASED IN CONNECTION WITH ANY SUCH AUDIT OR EVALUATION. In addition to the penalty established in section 2-3-103.7, any person who unlawfully releases confidential information shall be subject to any criminal or civil penalty under any applicable law for the unlawful release of the information.

SECTION 3. Act subject to petition - effective date. This act shall take effect at 12:01 a.m. on the day following the expiration of the ninety-day period after final adjournment of the general assembly (August 10, 2011, if adjournment sine die is on May 11, 2011); except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within such period, then the act, item, section, or part shall not take effect

unless approved by the people at the general election to be held in November 2012 and shall take effect on the date of the official declaration of the vote thereon by the governor.

Approved: April 13, 2011