HOUSE OF REPRESENTATIVES - FLOOR VERSION

STATE OF OKLAHOMA

2nd Session of the 54th Legislature (2014)

COMMITTEE SUBSTITUTE
FOR
HOUSE BILL NO. 2669 By: Derby

COMMITTEE SUBSTITUTE

An Act relating to information technology; amending 62 O.S. 2011, Section 34.32, as amended by Section 364, Chapter 304, O.S.L. 2012 (62 O.S. Supp. 2013, Section 34.32), which relates to standard risk assessments of state agencies; modifying requirement for a state agency to conduct an information security risk assessment; requiring risk assessment to be conducted by a third party; providing exception for certain state agencies; directing the Information Services Division of the Office of Management and Enterprise Services to approve certain number of firms; requiring certain state agencies to submit a final report; deleting certain penalty; deleting criteria for risk assessments; amending 62 O.S. 2011, Section 35.9, as last amended by Section 25, Chapter 358, O.S.L. 2013 (62 O.S. Supp. 2013, Section 35.9), which relates to quarterly progress reports under the Information Technology Consolidation and Coordination Act; adding certain information to report; providing an effective date; and declaring an emergency.

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

UNDERLINED language denotes Amendments to present Statutes.
BOLD FACE CAPITALIZED language denotes Committee Amendments.
~~Strike thru~~ language denotes deletion from present Statutes.

SECTION 1. AMENDATORY 62 O.S. 2011, Section 34.32, as amended by Section 364, Chapter 304, O.S.L. 2012 (62 O.S. Supp. 2013, Section 34.32), is amended to read as follows:

Section 34.32 A. The Information Services Division of the Office of Management and Enterprise Services shall create a standard security risk assessment for state agency information technology systems that complies with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Information Technology - Code of Practice for Security Management (ISO/IEC ~~17799~~ 27002).

B. Each state agency that has an information technology system shall ~~annually conduct~~ obtain an information security risk assessment to identify vulnerabilities associated with the information system. ~~A~~ Unless a state agency has internal expertise to conduct the risk assessment and can submit certification of such expertise along with the annual information security risk assessment, the risk assessment shall be conducted by a third party. The Information Services Division of the Office of Management and Enterprise Services shall approve not less than two firms which state agencies may choose from to conduct the information security risk assessment. A state agency with an information technology system that is not consolidated under the Information Technology Consolidation and Coordination Act or that is otherwise retained by the agency shall submit a final report of the information security

UNDERLINED language denotes Amendments to present Statutes.
BOLD FACE CAPITALIZED language denotes Committee Amendments.
~~Strike thru~~ language denotes deletion from present Statutes.

risk assessment ~~shall be submitted by each state agency~~ to the Information Services Division by the first day of December of each year. The final information security risk assessment report shall identify, prioritize, and document information security vulnerabilities for each of the state agencies assessed. ~~Failure to comply with the requirements of this subsection may result in funding being withheld from the agency. State agencies shall use either the standard security risk assessment created by the Information Services Division or a third-party risk assessment meeting the ISO/IEC 17799 standards and using the National Institute of Standards and Technology Special Publication 800-30 (NIST SP800-30) process and approved by the Information Services Division. The Information Services Division shall approve not less than two firms which state agencies may choose from to conduct the information security risk assessment.~~

C. The Information Services Division shall report the results of the state agency assessments required pursuant to this section to the Governor, the Speaker of the House of Representatives, and the President Pro Tempore of the Senate by the first day of January of each year.

SECTION 2. AMENDATORY 62 O.S. 2011, Section 35.9, as last amended by Section 25, Chapter 358, O.S.L. 2013 (62 O.S. Supp. 2013, Section 35.9), is amended to read as follows:

UNDERLINED language denotes Amendments to present Statutes.
BOLD FACE CAPITALIZED language denotes Committee Amendments.
~~Strike thru~~ language denotes deletion from present Statutes.

Section 35.9 In addition to any other reporting requirements required by law, the Chief Information Officer shall submit quarterly progress reports to the Director of the Office of Management and Enterprise Services, the Speaker of the House of Representatives and the President Pro Tempore of the Senate. The reports shall be submitted not later than January 31, April 30, July 31 and October 31 of each year and shall include, but not be limited to, the following information:

1. The status of the implementation of the plan of action required in paragraph 2 of subsection D of Section 34.11.1 of this title;

2. A list of information technology assets and positions transferred to the Information Services Division of the Office of Management and Enterprise Services pursuant to the provisions of subsection C of Section 35.5 of this title;

3. After July 1, 2012, and until the information technology consolidation is completed, an annual reduction of three percent (3%) in operational information technology and telecommunications expenditures realized in the aggregate by all consolidated state agencies;

4. A list of all state agencies which are not using the shared services as required in Section 35.6 of this title;

5. A list of all exemptions or extensions granted pursuant to the provisions of Section 35.7 of this title; ~~and~~

UNDERLINED language denotes Amendments to present Statutes.
BOLD FACE CAPITALIZED language denotes Committee Amendments.
~~Strike thru~~ language denotes deletion from present Statutes.

6. An accounting of the open source information technology assets of the state, including a description of any new open source assets deployed within the previous reporting period; and

7. Any other information as deemed appropriate by the Chief Information Officer.

SECTION 3. This act shall become effective July 1, 2014.

SECTION 4. It being immediately necessary for the preservation of the public peace, health and safety, an emergency is hereby declared to exist, by reason whereof this act shall take effect and be in full force from and after its passage and approval.

COMMITTEE REPORT BY: COMMITTEE ON GOVERNMENT MODERNIZATION, dated 02/24/2014 - DO PASS, As Amended.

UNDERLINED language denotes Amendments to present Statutes.
BOLD FACE CAPITALIZED language denotes Committee Amendments.
~~Strike thru~~ language denotes deletion from present Statutes.