An Act

ENROLLED SENATE
BILL NO. 584

By: Stanislawski of the Senate

and

Ortega of the House

An Act relating to public finance; amending 62 O.S. 2011, Section 34.32, as last amended by Section 1, Chapter 285, O.S.L. 2014 (62 O.S. Supp. 2018, Section 34.32), which relates to Security Risk Assessments; eliminating certain exception; establishing requirement for information security audit conducted by certain firm under certain basis; requiring submission of information security audit findings; modifying requirement for submission of findings within certain time; requiring submission of a list of remedies and a timeline for the repair of any deficiencies within certain time; permitting the Information Services Division to assist in repairing vulnerabilities; modifying reporting requirements; requiring technology system consolidation under certain circumstance; providing exception for certain agencies and institutions subject to certain mandatory cybersecurity standards and information security controls; and providing an effective date.

SUBJECT: State agency information technology systems

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

SECTION 1. AMENDATORY 62 O.S. 2011, Section 34.32, as last amended by Section 1, Chapter 285, O.S.L. 2014 (62 O.S. Supp. 2018, 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 27002).

B. Each state agency that has an information technology system shall obtain an information security risk assessment to identify vulnerabilities associated with the information system~~. 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.

C. 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 additionally be required to have an information security audit conducted by a firm approved by the Information Services Division that is based upon the most current version of the NIST Cyber-Security Framework, and shall submit a final report of the information security risk assessment and information security audit findings to the Information Services Division ~~by the first day of December of~~ each year on a schedule set by the Information Services Division. Agencies shall also submit a list of remedies and a timeline for the repair of any deficiencies to the Information Services Division within ten (10) days of the completion of the audit. The final information security risk assessment report shall identify, prioritize, and document information security vulnerabilities for each of the state agencies assessed. The Information Services Division may assist agencies in repairing any vulnerabilities to ensure compliance in a timely manner.

~~C. The~~ D. Subject to the provisions of subsection C of Section 34.12 of this title, the Information Services Division shall report the results of the state agency assessments and information security audit findings 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. Any state agency with an information technology system that is not consolidated under the Information Technology Consolidation and Coordination Act that cannot comply with the provisions of this section shall consolidate under the Information Technology Consolidation and Coordination Act.

E. This act shall not apply to state agencies subject to mandatory North American Electric Reliability Corporation (NERC) cybersecurity standards and institutions within The Oklahoma State System of Higher Education, the Oklahoma State Regents for Higher Education and the telecommunications network known as OneNet that follow the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)-Security techniques-Code of Practice for Information Security Controls or National Institute of Standards and Technology.

SECTION 2. This act shall become effective November 1, 2019.

Passed the Senate the 2nd day of May, 2019.

_____
Presiding Officer of the Senate

Passed the House of Representatives the 23rd day of April, 2019.

_____
Presiding Officer of the House
of Representatives

OFFICE OF THE GOVERNOR

Received by the Office of the Governor this _____

day of _____, 20_____, at _____ o'clock _____ M.

By: _____

Approved by the Governor of the State of Oklahoma this _____

day of _____, 20_____, at _____ o'clock _____ M.

_____
Governor of the State of Oklahoma

OFFICE OF THE SECRETARY OF STATE

Received by the Office of the Secretary of State this _____

day of _____, 20 _____, at _____ o'clock _____ M.

By: _____