

1 ENGROSSED HOUSE AMENDMENTS

TO

2 ENGROSSED SENATE BILL NO. 584

By: Stanislawski of the Senate

3 and

4 Ortega of the House

5

6

7 An Act relating to public finance; amending 62 O.S.
8 2011, Section 34.32, as last amended by Section 1,
9 Chapter 285, O.S.L. 2014 (62 O.S. Supp. 2018, Section
10 34.32), which relates to Security Risk Assessments;
11 eliminating certain exception; establishing
12 requirement for information security audit conducted
13 by certain firm under certain basis; requiring
14 submission of information security audit findings;
15 modifying requirement for submission of findings
16 within certain time; requiring submission of a list
17 of remedies and a timeline for the repair of any
18 deficiencies within certain time; requiring the
19 Information Services Division to assist in repairing
20 vulnerabilities; modifying reporting requirements;
21 requiring technology system consolidation under
22 certain circumstance; providing exception for certain
23 agencies subject to certain mandatory cybersecurity
24 standards; and providing an effective date.

18 AMENDMENT NO. 1. Page 1, strike the title

19 AMENDMENT NO. 2. Page 3, line 20, after the word "standards" and
20 before the period "." insert the following
language

21 "and institutions within The Oklahoma State System of Higher
22 Education, the Oklahoma State Regents for Higher Education and the
23 telecommunications network known as OneNet that follow the
24 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"

1 AMENDMENT NO. 3. Page 1, restore the title

2 AMENDMENT NO. 4. Page 2, line 13, after the period "." and before
3 the capitalized word "A", insert the capital
4 letter "C."

5 Page 2, line 22, after the word "year" and before
6 the period ".", insert the following language:
7 "on a schedule set by the Information Services
8 Division"

9 Page 3, line 4, delete the word "shall" and insert
10 in lieu thereof the word "may"

11 Page 3, line 7, strike existing "C." and insert in
12 lieu thereof "D."

13 Page 3, line 18, reletter existing subsection "D."
14 as subsection "E."

15 and amend title to conform

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

17

18

19 _____
20 Presiding Officer of the House of
21 Representatives

22 Passed the Senate the ____ day of _____, 2019.

23

24

25 _____
26 Presiding Officer of the Senate

27

28

29

30

1 ENGROSSED SENATE
2 BILL NO. 584

By: Stanislawski of the Senate

3 and

4 Ortega of the House

5
6 An Act relating to public finance; amending 62 O.S.
7 2011, Section 34.32, as last amended by Section 1,
8 Chapter 285, O.S.L. 2014 (62 O.S. Supp. 2018, Section
9 34.32), which relates to Security Risk Assessments;
10 eliminating certain exception; establishing
11 requirement for information security audit conducted
12 by certain firm under certain basis; requiring
13 submission of information security audit findings;
14 modifying requirement for submission of findings
15 within certain time; requiring submission of a list
16 of remedies and a timeline for the repair of any
17 deficiencies within certain time; requiring the
18 Information Services Division to assist in repairing
19 vulnerabilities; modifying reporting requirements;
20 requiring technology system consolidation under
21 certain circumstance; providing exception for certain
22 agencies subject to certain mandatory cybersecurity
23 standards; and providing an effective date.

24 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

1 Standardization (ISO) and the International Electrotechnical
2 Commission (IEC) Information Technology - Code of Practice for
3 Security Management (ISO/IEC 27002).

4 B. Each state agency that has an information technology system
5 shall obtain an information security risk assessment to identify
6 vulnerabilities associated with the information system. ~~Unless a~~
7 ~~state agency has internal expertise to conduct the risk assessment~~
8 ~~and can submit certification of such expertise along with the annual~~
9 ~~information security risk assessment, the risk assessment shall be~~
10 ~~conducted by a third party.~~ The Information Services Division of
11 the Office of Management and Enterprise Services shall approve not
12 less than two firms which state agencies may choose from to conduct
13 the information security risk assessment. A state agency with an
14 information technology system that is not consolidated under the
15 Information Technology Consolidation and Coordination Act or that is
16 otherwise retained by the agency shall additionally be required to
17 have an information security audit conducted by a firm approved by
18 the Information Services Division that is based upon the most
19 current version of the NIST Cyber-Security Framework, and shall
20 submit a final report of the information security risk assessment
21 and information security audit findings to the Information Services
22 Division ~~by the first day of December of~~ each year. Agencies shall
23 also submit a list of remedies and a timeline for the repair of any
24 deficiencies to the Information Services Division within ten (10)

1 days of the completion of the audit. The final information security
2 risk assessment report shall identify, prioritize, and document
3 information security vulnerabilities for each of the state agencies
4 assessed. The Information Services Division shall assist agencies
5 in repairing any vulnerabilities to ensure compliance in a timely
6 manner.

7 C. The Subject to the provisions of subsection C of Section
8 34.12 of this title, the Information Services Division shall report
9 the results of the state agency assessments and information security
10 audit findings required pursuant to this section to the Governor,
11 the Speaker of the House of Representatives, and the President Pro
12 Tempore of the Senate by the first day of January of each year. Any
13 state agency with an information technology system that is not
14 consolidated under the Information Technology Consolidation and
15 Coordination Act that cannot comply with the provisions of this
16 section shall consolidate under the Information Technology
17 Consolidation and Coordination Act.

18 D. This act shall not apply to state agencies subject to
19 mandatory North American Electric Reliability Corporation (NERC)
20 cybersecurity standards.

21 SECTION 2. This act shall become effective November 1, 2019.
22
23
24

