

1 **SENATE FLOOR VERSION**

2 March 26, 2014

3 COMMITTEE SUBSTITUTE
4 FOR ENGROSSED
5 HOUSE BILL NO. 2669

By: Derby of the House

and

Brinkley of the Senate

6
7
8
9 [information technology - assessments of state
10 agencies - information security risk assessment -
11 final report - effective date -
12 emergency]

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

14 SECTION 1. AMENDATORY 62 O.S. 2011, Section 34.32, as
15 amended by Section 364, Chapter 304, O.S.L. 2012 (62 O.S. Supp.
16 2013, Section 34.32), is amended to read as follows:

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

1 B. Each state agency that has an information technology system
2 shall ~~annually conduct~~ obtain an information security risk
3 assessment to identify vulnerabilities associated with the
4 information system. A Unless a state agency has internal expertise
5 to conduct the risk assessment and can submit certification of such
6 expertise along with the annual information security risk
7 assessment, the risk assessment shall be conducted by a third party.
8 The Information Services Division of the Office of Management and
9 Enterprise Services shall approve not less than two firms which
10 state agencies may choose from to conduct the information security
11 risk assessment. A state agency with an information technology
12 system that is not consolidated under the Information Technology
13 Consolidation and Coordination Act or that is otherwise retained by
14 the agency shall submit a final report of the information security
15 ~~risk assessment shall be submitted by each state agency to the~~
16 Information Services Division by the first day of December of each
17 year. The final information security risk assessment report shall
18 identify, prioritize, and document information security
19 vulnerabilities for each of the state agencies assessed. ~~Failure to~~
20 ~~comply with the requirements of this subsection may result in~~
21 ~~funding being withheld from the agency. State agencies shall use~~
22 ~~either the standard security risk assessment created by the~~
23 ~~Information Services Division or a third-party risk assessment~~
24 ~~meeting the ISO/IEC 17799 standards and using the National Institute~~

1 ~~of Standards and Technology Special Publication 800-30 (NIST SP800-~~
2 ~~30) process and approved by the Information Services Division. The~~
3 ~~Information Services Division shall approve not less than two firms~~
4 ~~which state agencies may choose from to conduct the information~~
5 ~~security risk assessment.~~

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

11 SECTION 2. This act shall become effective July 1, 2014.

12 SECTION 3. It being immediately necessary for the preservation
13 of the public peace, health and safety, an emergency is hereby
14 declared to exist, by reason whereof this act shall take effect and
15 be in full force from and after its passage and approval.

16 COMMITTEE REPORT BY: COMMITTEE ON APPROPRIATIONS
17 March 26, 2014 - DO PASS AS AMENDED

18
19
20
21
22
23
24