§ 143B-1377. State CIO approval of security standards and risk assessments.

(a) Notwithstanding G.S. 143-48.3, 143B-1320(b), or 143B-1320(c), or any other provision of law, and except as otherwise provided by this Article, all information technology security goods, software, or services purchased using State funds, or for use by a State agency or in a State facility, shall be subject to approval by the State CIO in accordance with security standards adopted under this Part.

(b) The State CIO shall conduct risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies. The State CIO may contract with another party or parties to perform the assessments. Detailed reports of the risk and security issues identified shall be kept confidential as provided in G.S. 132-6.1(c).

(c) If the legislative branch or the judicial branch develop their own security standards, taking into consideration the mission and functions of that entity, that are comparable to or exceed those set by the State CIO under this section, then those entities may elect to be governed by their own respective security standards. In these instances, approval of the State CIO shall not be required before the purchase of information technology security devices and services. If requested, the State CIO shall consult with the legislative branch and the judicial branch in reviewing the security standards adopted by those entities.

(d) Before a State agency may enter into any contract with another party for an assessment of network vulnerability, the State agency shall notify the State CIO and obtain approval of the request. If the State agency enters into a contract with another party for assessment and testing, after approval of the State CIO, the State agency shall issue public reports on the general results of the reviews. The contractor shall provide the State agency with detailed reports of the security issues identified that shall not be disclosed as provided in G.S. 132-6.1(c). The State agency shall provide the State CIO with copies of the detailed reports that shall not be disclosed as provided in G.S. 132-6.1(c).

(e) Nothing in this section shall be construed to preclude the Office of the State Auditor from assessing the security practices of State information technology systems as part of its statutory duties and responsibilities. (2015-241, s. 7A.2.)