Article 15.

Department of Information Technology.

Part 1. General Provisions.

§ 143B-1320. Definitions; scope; exemptions.

(a) Definitions. – The following definitions apply in this Article:

(1) CGIA. – Center for Geographic Information and Analysis.

(2) Repealed by Session Laws 2021-180, s. 19A.7A(d), effective January 1, 2022.

(3) Community of practice. – A collaboration of organizations with similar requirements, responsibilities, or interests.

(4) Cooperative purchasing agreement. – An agreement between a vendor and one or more states or state agencies providing that the parties may collaboratively or collectively purchase information technology goods and services in order to increase economies of scale and reduce costs.

(4a) Cybersecurity incident. – An occurrence that:

a. Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.

(5) Department. – The Department of Information Technology.

(6) Distributed information technology assets. – Hardware, software, and communications equipment not classified as traditional mainframe-based items, including personal computers, local area networks, servers, mobile computers, peripheral equipment, and other related hardware and software items.

(7) Enterprise solution. – An information technology solution that can be used by multiple agencies.

(8) Exempt agencies. – An entity designated as exempt in subsection (b) of this section.

(9) GDAC. – Government Data Analytics Center.

(10) GICC. – North Carolina Geographic Information Coordinating Council.

(11) Information technology or IT. – Set of tools, processes, and methodologies, including, but not limited to, coding and programming; data communications, data conversion, and data analysis; architecture; planning; storage and retrieval; systems analysis and design; systems control; mobile applications; and equipment and services employed to collect, process, and present information to support the operation of an organization. The term also includes office automation, multimedia, telecommunications, and any personnel and support personnel required for planning and operations.

(12) Recodified as subdivision (a)(4a) at the direction of the Revisor of Statutes.

(13) Local government entity. – A local political subdivision of the State, including a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

(14) Participating agency. – Any agency that has transferred its information technology personnel, operations, projects, assets, and funding to the Department of Information Technology. The State CIO shall be responsible

for providing all required information technology support to participating agencies.

(14a) Ransomware attack. – A cybersecurity incident where a malicious actor introduces software into an information system that encrypts data and renders the systems that rely on that data unusable, followed by a demand for a ransom payment in exchange for decryption of the affected data.

(15) Recodified as subdivision (a)(16a) at the direction of the Revisor of Statutes.

(16) Separate agency. – Any agency that has maintained responsibility for its information technology personnel, operations, projects, assets, and funding. The agency head shall work with the State CIO to ensure that the agency has all required information technology support.

(16a) Significant cybersecurity incident. – A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:

1. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or

2. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

b. Incidents that involve information that is not recoverable or cannot be recovered within defined time lines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.

(17) State agency or agency. – Any agency, department, institution, commission, committee, board, division, bureau, office, unit, officer, or official of the State. The term does not include the legislative or judicial branches of government or The University of North Carolina.

(18) State Chief Information Officer or State CIO. – The head of the Department, who is a Governor's cabinet level officer.

(19) State CIO approved data center. – A data center designated by the State CIO for State agency use that meets operational standards established by the Department.

(b) Exemptions. – Except as otherwise specifically provided by law, the provisions of this Chapter do not apply to the following entities: the General Assembly, the Judicial Department, and The University of North Carolina and its constituent institutions. These entities may elect to participate in the information technology programs, services, or contracts offered by the Department, including information technology procurement, in accordance with the statutes, policies, and rules of the Department. The election must be made in writing, as follows:

(1) For the General Assembly, by the Legislative Services Commission.

(2) For the Judicial Department, by the Chief Justice.

(3) For The University of North Carolina, by the Board of Governors.

(4) For the constituent institutions of The University of North Carolina, by the respective boards of trustees.

(c) Deviations. – Any State agency may apply in writing to the State Chief Information Officer for approval to deviate from the provisions of this Chapter. If granted by the State Chief Information Officer, any deviation shall be consistent with available appropriations and shall be subject to such terms and conditions as may be specified by the State CIO.

(d) Review. – Notwithstanding subsection (b) of this section, any State agency shall review and evaluate any deviation authorized and shall, in consultation with the Department of Information Technology, adopt a plan to phase out any deviations that the State CIO determines to be unnecessary in carrying out functions and responsibilities unique to the agency having a deviation. The plan adopted by the agency shall include a strategy to coordinate its general information processing functions with the Department of Information Technology in the manner prescribed by this act and provide for its compliance with policies, procedures, and guidelines adopted by the Department of Information Technology. Any agency receiving a deviation shall submit its plan to the Office of State Budget and Management as directed by the State Chief Information Officer. (2015-241, s. 7A.2(b); 2019-200, s. 6(d); 2021-180, ss. 19A.7A(d), 38.13(b).)