

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) CJIN. – Criminal Justice Information Network.
  - (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.
  - (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) Information technology security incident. – A computer-, network-, or paper-based activity that results directly or indirectly in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data.
  - (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.

- (15) Security incident. A warning or indication of a threat to or breach of information or computer security. The term also includes threats that have already occurred.
- (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.
- (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).)

**§ 143B-1321. Powers and duties of the Department; cost-sharing with exempt entities.**

- (a) The Department shall have the following powers and duties:
  - (1) Provide information technology support and services to State agencies.

- (2) Provide such information technology support to local government entities and others, as may be required.
- (3) Establish and document the strategic direction of information technology in the State.
- (4) Assist State agencies in meeting their business objectives.
- (5) Plan and coordinate information technology efforts with State agencies, nonprofits, and private organizations, as required.
- (6) Establish a consistent process for planning, maintaining, and acquiring the State's information technology resources. This includes responsibility for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources.
- (7) Develop standards and accountability measures for information technology projects, including criteria for effective project management.
- (8) Set technical standards for information technology, review and approve information technology projects and budgets, establish and enforce information technology security standards, establish and enforce standards for the procurement of information technology resources, and develop a schedule for the replacement or modification of information technology systems.
- (9) Implement enterprise procurement processes and develop metrics to support this process.
- (10) Manage the information technology funding for State agencies, to include the Information Technology Fund for statewide information technology efforts and the Information Technology Internal Service Fund for agency support functions.
- (11) Support, maintain, and develop metrics for the State's technology infrastructure and facilitate State agencies' delivery of services to citizens.
- (12) Operate as the State enterprise organization for information technology governance.
- (13) Advance the State's technology and data management capabilities.
- (14) Prepare and present the Department's budget in accordance with Chapter 143C of the General Statutes, the State Budget Act.
- (15) Obtain, review, and maintain, on an ongoing basis, records of the appropriations, allotments, expenditures, revenues, grants, and federal funds for each State agency for information technology.
- (16) Adopt rules for the administration of the Department and implementing this Article, pursuant to the Administrative Procedure Act, Chapter 150B of the General Statutes.
- (17) Require reports by State agencies, departments, and institutions about information technology assets, systems, personnel, and projects and prescribing the form of such reports.
- (18) Prescribe the manner in which information technology assets, systems, and personnel shall be provided and distributed among agencies, to include changing the distribution when the State CIO determines that is necessary.
- (19) Prescribe the manner of inspecting or testing information technology assets, systems, or personnel to determine compliance with information technology plans, specifications, and requirements.

- (20) Submit all rates and fees for common, shared, and State government-wide technology services provided by the Department to the Office of State Budget and Management for approval.
- (21) Establish and operate, or delegate operations of, centers of expertise (COE) for specific information technologies and services to serve two or more agencies on a cost-sharing basis, if the State CIO, after consultation with the Office of State Budget and Management, decides it is advisable from the standpoint of efficiency and economy to establish these centers and services.
- (22) Identify and develop projects to facilitate the consolidation of information technology equipment, support, and projects.
- (23) Identify an agency to serve as the lead (COE) for an enterprise effort, when appropriate.
- (24) Require any State agency served to transfer to the Department or COE ownership, custody, or control of information-processing equipment, software, supplies, positions, and support required by the shared centers and services.
- (25) Charge each State agency for which services are performed its proportionate part of the cost of maintaining and operating the shared centers and services, subject to approval by the Office of State Budget and Management.
- (26) Develop performance standards for shared services in coordination with supported State agencies and publish performance reports on the Department Web site.
- (27) Adopt plans, policies, and procedures for the acquisition, management, and use of information technology resources in State agencies to facilitate more efficient and economic use of information technology in the agencies.
- (28) Develop and manage career progressions and training programs to efficiently implement, use, and manage information technology resources throughout State government.
- (29) Provide local government entities with access to the Department's services as authorized in this section for State agencies. Access shall be provided on the same cost basis that applies to State agencies.
- (30) Support the operation of the CGIA, GICC, GDAC, CJIN, and 911 Board.
- (31) Repealed by Session Laws 2016-94, s. 7.14(d), effective July 1, 2016.
- (32) Provide geographic information systems services through the Center for Geographic Information and Analysis on a cost recovery basis. The Department and the Center for Geographic Information and Analysis may contract for funding from federal or other sources to conduct or provide geographic information systems services for public purposes.
- (33) Support the development, implementation, and operation of an Education Community of Practice.

(b) Cost-Sharing with Other Branches. – Notwithstanding any other provision of law to the contrary, the Department shall provide information technology services on a cost-sharing basis to exempt agencies, upon request. (2015-241, s. 7A.2(b); 2016-94, s. 7.14(d).)

**§ 143B-1322. State CIO duties; Departmental personnel and administration.**

(a) State CIO. – The State Chief Information Officer (State CIO) is the head of the Department, a member of the Governor's cabinet, and may also be referred to as the Secretary of the Department of Information Technology. The State CIO is appointed by and serves at the pleasure of the Governor. The State CIO shall be qualified by education and experience for the office. The salary of the State CIO shall be set by the Governor. The State CIO shall receive longevity pay on the same basis as is provided to employees of the State who are subject to the North Carolina Human Resources Act.

(b) Departmental Personnel. – The State CIO may appoint one or more deputy State CIOs, each of whom shall be under the direct supervision of the State CIO. The salaries of the deputy State CIOs shall be set by the State CIO. The State CIO and the Deputy State CIOs are exempt from the North Carolina Human Resources Act. Subject to the approval of the Governor and limitations of the G.S. 126-5, the State CIO may appoint or designate additional managerial and policy making positions, including, but not limited to, the Department's chief financial officer and general counsel, each of whom shall be exempt from the North Carolina Human Resources Act.

(c) Administration. – The Department shall be managed under the administration of the State CIO. The State CIO shall have the following powers and duty to do all of the following:

- (1) Ensure that executive branch agencies receive all required information technology support in an efficient and timely manner.
- (2) Ensure that such information technology support is provided to local government entities and others, as appropriate.
- (3) Approve the selection of the respective agency chief information officers.
- (4) As required, plan and coordinate information technology efforts with State agencies, nonprofits, and private organizations.
- (5) Ensure the security of State information technology systems and networks, as well as associated data, developing standardized systems and processes.
- (6) Prepare and present the Department's budget in accordance with Chapter 143C of the General Statutes, the State Budget Act.
- (7) Establish rates for all goods and services provided by the Department within required schedules.
- (8) Identify and work to consolidate duplicate information technology capabilities.
- (9) Identify and develop plans to increase State data center efficiencies, consolidating assets in State-managed data centers.
- (10) Plan for and manage State network development and operations.
- (11) Centrally classify, categorize, manage, and protect the State's data.
- (12) Obtain, review, and maintain, on an ongoing basis, records of the appropriations, allotments, expenditures, and revenues of each State agency for information technology.
- (13) Be responsible for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources.
- (14) Set technical standards for information technology, review and approve information technology projects and budgets, establish information technology security standards, provide for the procurement of information

technology resources, and develop a schedule for the replacement or modification of information technology systems.

- (15) Require reports by State departments, institutions, or agencies of information technology assets, systems, personnel, and projects; prescribe the form of such reports; and verify the information when the State CIO determines verification is necessary.
- (16) Prescribe the manner in which information technology assets, systems, and personnel shall be provided and distributed among agencies.
- (17) Establish and maintain a program to provide career management for information technology professionals.
- (18) Prescribe the manner of inspecting or testing information technology assets, systems, or personnel to determine compliance with information technology plans, specifications, and requirements.
- (19) Supervise and support the operations of the CGIA, GICC, GDAC, CJIN, and 911 Board.
- (20) Oversee and coordinate an Education Community of Practice.
- (21) Repealed by Session Laws 2016-94, s. 7.14(d), effective July 1, 2016.

(d) **Budgetary Matters.** – The Department's budget shall incorporate information technology costs and anticipated expenditures of State agencies identified as participating agencies, together with all divisions, boards, commissions, or other State entities for which the principal departments have budgetary authority.

(e) **State Ethics Act.** – All employees of the Department shall be subject to the applicable provisions of the State Government Ethics Act under Chapter 138A of the General Statutes. (2015-241, s. 7A.2(b); 2015-268, s. 2.2; 2016-94, s. 7.14(d); 2016-96, s. 1.)

**§ 143B-1323. Departmental organization; divisions and units; education community of practice.**

(a) **Organization.** – The Department shall be organized by the State CIO into divisions and units that support its duties.

(b) **Education Community of Practice.** – There is established an Education Community of Practice to promote collaboration and create efficiencies between and among The University of North Carolina and its constituent institutions, the North Carolina Community Colleges System Office, the constituent institutions of the Community College System, the Department of Public Instruction, and local school administrative units.

(c) **Other Units.** – Other units of the Department include the following:

- (1) Center for Geographic Information and Analysis.
- (2) Criminal Justice Information Network.
- (3) Government Data Analytics Center.
- (4) North Carolina 911 Board.
- (5) North Carolina Geographic Information Coordinating Council. (2015-241, s. 7A.2(b).)

**§ 143B-1324. State agency information technology management; deviations for State agencies.**

Each State agency shall have tools and applications specific to their respective functions in order to effectively and efficiently carry out the business of the State with respect to all of the following:

- (1) Administrative support.
- (2) Facilities management.
- (3) Internal auditing.
- (4) Boards administration.
- (5) Departmental policies and procedures. (2015-241, s. 7A.2(b).)

**§ 143B-1325. Transition to Department of Information Technology.**

(a) Transition Period. – During the 2015-2016 fiscal year, the State CIO shall work with appropriate State agencies to develop a State business plan. The State CIO shall develop documentation to support the consolidation of enterprise information technology functions within the executive branch to include the following:

- (1) Information technology architecture.
- (2) Updated State information technology strategic plan that reflects State and agency business plans and the State information technology architecture.
- (3) Information technology funding process to include standardized, transparent rates that reflect market costs for information technology requirements.
- (4) Information technology personnel management.
- (5) Information technology project management.
- (6) Information technology procurement.
- (7) Hardware configuration and management.
- (8) Software acquisition and management.
- (9) Data center operations.
- (10) Network operations.
- (11) System and data security, including disaster recovery.

(b) Phased Transitions. – The State CIO shall develop detailed plans for the phased transition of participating agencies to the Department, as well as a plan that defines in detail how information technology support shall be provided to agencies that are not participating agencies. These plans shall be coordinated, in writing, with each agency and shall address any issues unique to a specific agency.

(c) Participating Agencies. – The State CIO shall prepare detailed plans to transition each of the participating agencies. As the transition plans are completed, the following participating agencies shall transfer information technology personnel, operations, projects, assets, and appropriate funding to the Department of Information Technology:

- (1) Department of Natural and Cultural Resources.
- (2) Department of Health and Human Services.
- (3) Department of Revenue.
- (4) Department of Environmental Quality.
- (5) Department of Transportation.
- (6) Department of Administration.
- (7) Department of Commerce.
- (8) Governor's Office.
- (9) Office of State Budget and Management.
- (10) Office of State Human Resources.

- (11) Repealed by Session Laws 2016-94, s. 7.11(a), effective July 1, 2016.
- (12) Department of Military and Veterans Affairs.
- (13) Department of Public Safety, with the exception of the following:
  - a. State Bureau of Investigation.
  - b. State Highway Patrol.
  - c. Division of Emergency Management.

The State CIO shall ensure that agencies' operations are not adversely impacted during the transition.

(d) Report on Transition Planning. – The Community College System Office and the State Board of Elections shall work with the State CIO to plan their transition to the Department. By October 1, 2018, these agencies, in conjunction with the State CIO, shall report to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division on their respective transition plans.

(e) Separate agencies may transition their information technology to the Department following completion of a transition plan. (2015-241, s. 7A.2(b); 2015-268, s. 2.8; 2016-94, s. 7.11(a).)

§ 143B-1326: Reserved for future codification purposes.

§ 143B-1327: Reserved for future codification purposes.

§ 143B-1328: Reserved for future codification purposes.

§ 143B-1329: Reserved for future codification purposes.

Part 2. Information Technology Planning, Funding, and Reporting.

§ 143B-1330. **Planning and financing State information technology resources.**

(a) The State CIO shall develop policies for agency information technology planning and financing. Agencies shall prepare and submit such plans as required in this section, as follows:

- (1) The Department shall analyze the State's legacy information technology systems and develop a plan to document the needs and costs for replacement systems, as well as determining and documenting the time frame during which State agencies can continue to efficiently use legacy information technology systems, resources, security, and data management to support their operations. The plan shall include an inventory of legacy applications and infrastructure, required capabilities not available with the legacy system, the process, time line, and cost to migrate from legacy environments, and any other information necessary for fiscal or technology planning. The State CIO shall have the authority to prioritize the upgrade and replacement of legacy systems. Agencies shall provide all requested documentation to validate reporting on legacy systems and shall make the systems available for inspection by the Department.
- (2) The State CIO shall develop a biennial State Information Technology Plan (Plan), including, but not limited to, the use of cloud-based utility computing for use by State agencies.

- (3) The State CIO shall develop one or more strategic plans for information technology. The State CIO shall determine whether strategic plans are needed for any agency and shall consider an agency's operational needs, functions, and capabilities when making such determinations.

(b) Based on requirements identified during the strategic planning process, the Department shall develop and transmit to the General Assembly the biennial State Information Technology Plan in conjunction with the Governor's budget of each regular session. The Plan shall include the following elements:

- (1) Anticipated requirements for information technology support over the next five years.
- (2) An inventory of current information technology assets and major projects. As used in this subdivision, the term "major project" includes projects costing more than five hundred thousand dollars (\$500,000) to implement.
- (3) Significant unmet needs for information technology resources over a five-year time period. The Plan shall rank the unmet needs in priority order according to their urgency.
- (4) A statement of the financial requirements, together with a recommended funding schedule and funding sources for major projects and other requirements in progress or anticipated to be required during the upcoming fiscal biennium.
- (5) An analysis of opportunities for statewide initiatives that would yield significant efficiencies or improve effectiveness in State programs.
- (6) As part of the plan, the State CIO shall develop and periodically update a long-range State Information Technology Plan that forecasts, at a minimum, the needs of State agencies for the next 10 years.

(c) Each participating agency shall actively participate in preparing, testing, and implementing an information technology plan required under subsection (b) of this section. Separate agencies shall prepare biennial information technology plans, including the requirements listed in subsection (b) of this section, and transmit these plans to the Department by a date determined by the State CIO in each even-numbered year. Agencies shall provide all financial information to the State CIO necessary to determine full costs and expenditures for information technology assets and resources provided by the agencies or through contracts or grants. The Department shall consult with and assist State agencies in the preparation of these plans; shall provide appropriate personnel or other resources to the participating agencies and to separate agencies upon request. Plans shall be submitted to the Department by a date determined by the State CIO in each even-numbered year. (2015-241, s. 7A.2(b); 2015-268, s. 2.11; 2016-94, s. 7.4(h).)

**§ 143B-1331. Business continuity planning.**

The State CIO shall oversee the manner and means by which information technology business and disaster recovery plans for the State agencies are created, reviewed, and updated. Each State agency shall establish a disaster recovery planning team to work with the Department, or other resources designated by the State CIO, to develop the disaster recovery plan and to administer implementation of the plan. In developing the plan, all of the following shall be completed:

- (1) Consider the organizational, managerial, and technical environments in which the disaster recovery plan must be implemented.
- (2) Assess the types and likely parameters of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.
- (3) List protective measures to be implemented in anticipation of a natural or man-made disaster.
- (4) Determine whether the plan is adequate to address information technology security incidents.

Each State agency shall submit its disaster recovery plan to the State CIO on an annual basis and as otherwise requested by the State CIO. (2015-241, s. 7A.2(b).)

#### **§ 143B-1332. Information Technology Fund.**

There is established a special revenue fund to be known as the Information Technology Fund, which may receive transfers or other credits as authorized by the General Assembly. Money may be appropriated from the Information Technology Fund to support the operation and administration that meet statewide requirements, including planning, project management, security, electronic mail, State portal operations, early adoption of enterprise efforts, and the administration of systemwide procurement procedures. Funding for participating agency information technology projects shall be appropriated to the Information Technology Fund and may be reallocated by the State CIO, if appropriate, following coordination with the impacted agencies and written approval by the Office of State Budget and Management. Any redirection of agency funds shall immediately be reported to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division with a detailed explanation of the reasons for the redirection. Expenditures involving funds appropriated to the Department from the Information Technology Fund shall be made by the State CIO. Interest earnings on the Information Technology Fund balance shall be credited to the Information Technology Fund. (2015-241, s. 7A.2(b).)

#### **§ 143B-1333. Internal Service Fund.**

(a) The Internal Service Fund is established within the Department as a fund to provide goods and services to State agencies on a cost-recovery basis. The Department shall establish fees for subscriptions and chargebacks for consumption-based services. The Information Technology Strategic Sourcing Office shall be funded through a combination of administrative fees as part of the IT Supplemental Staffing contract, as well as fees charged to agencies using their services. The State CIO shall establish and annually update consistent, fully transparent, easily understandable fees and rates that reflect industry standards for any good or service for which an agency is charged. These fees and rates shall be prepared by October 1 and shall be approved by the Office of State Budget and Management. The Office of State Budget and Management shall ensure that State agencies have the opportunity to adjust their budgets based on any rate or fee changes prior to submission of those budget recommendations to the General Assembly. The approved Information Technology Internal Service Fund budget and associated rates shall be included in the Governor's budget recommendations to the General Assembly.

(b) Repealed by Session Laws 2016-94, s. 7.4(d), effective July 1, 2016.

(c) Receipts shall be used solely for the purpose for which they were collected. In coordination with the Office of the State Controller and the Office of State Budget Management, the State CIO shall ensure processes are established to manage federal receipts, maximize those

receipts, and ensure that federal receipts are correctly utilized. (2015-241, s. 7A.2(b); 2016-94, s. 7.4(d).)

§ 143B-1334: Repealed by Session Laws 2016-94, s. 7.4(e), effective July 1, 2016.

**§ 143B-1335. Financial reporting and accountability for information technology investments and expenditures.**

The Department, along with the Office of State Budget and Management and the Office of the State Controller, shall develop processes for budgeting and accounting of expenditures for information technology operations, services, projects, infrastructure, and assets for State agencies, notwithstanding any exemptions or deviations permitted pursuant to G.S. 143B-1320(b) or (c). The budgeting and accounting processes may include hardware, software, personnel, training, contractual services, and other items relevant to information technology and the sources of funding for each. Annual reports regarding information technology shall be coordinated by the Department with the Office of State Budget and Management and the Office of the State Controller and submitted to the Governor and the General Assembly on or before October 1 of each year.

The State CIO shall not enter into any information technology contracts requiring agency financial participation without obtaining written agreement from participating agencies regarding apportionment of the contract costs.

The State CIO shall review the information technology budgets for participating agencies and shall recommend appropriate adjustments to support requirements identified by the State CIO. (2015-241, s. 7A.2(b).)

**§ 143B-1336. Information technology human resources.**

(a) The State CIO may appoint all employees of the Department necessary to carry out the powers and duties of the Department. All employees of the Department are under the supervision, direction, and control of the State CIO, who may assign any function vested in his or her office to any subordinate employee of the Department.

(b) The State CIO shall establish a detailed, standardized, systemic plan for the transition of participating agency personnel to the new organization. This shall include the following:

- (1) Documentation of current information technology personnel requirements.
- (2) An inventory of current agency information technology personnel and their skills.
- (3) Analysis and documentation of the gaps between current personnel and identified requirements.
- (4) An explanation of how the Department plans to fill identified gaps.
- (5) The Department's plan to eliminate positions no longer required.
- (6) The Department's plan for employees whose skills are no longer required.

For each person to be transferred, the State CIO shall identify a designated position with a job description, determine the cost for the position, identify funding sources, and establish a standardized rate.

(c) Participating agency information technology personnel performing information technology functions shall be moved to the Department. The State CIO shall consolidate participating agency information technology personnel following the time lines established in the

plans required by G.S. 143B-1325(b) once a detailed plan has been developed for transitioning the personnel to the new agency.

(d) The State CIO shall establish standard information technology career paths for both management and technical tracks, including defined qualifications, career progression, training requirements, and appropriate compensation. For information technology procurement professionals, the State CIO shall establish a career path that includes defined qualifications, career progression, training requirements, and appropriate compensation. These career paths shall be documented by February 1, 2016, and shall be provided to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division by February 1, 2016, but may be submitted incrementally to meet Department requirements. The career paths shall be updated on an annual basis.

(e) Any new positions established by the Department shall be exempt from the North Carolina Human Resources Act; provided, however, that nonexempt employees transferred from participating agencies to a newly established position in the Department shall not become exempt solely by virtue of that transfer.

(f) The State CIO may, subject to the provisions of G.S. 147-64.7(b)(2), obtain the services of independent public accountants, qualified management consultants, and other professional persons or experts to carry out the powers and duties of this Article if the Department does not have any personnel qualified to perform the function for which the professionals would be engaged and if the requirement has been included in the Department's budget for the year in which the services are required.

(g) Criminal Records Checks. – The State CIO shall require background investigations of any employee or prospective employee, including a criminal history record check, which may include a search of the State and National Repositories of Criminal Histories based on the person's fingerprints. A criminal history record check shall be conducted by the State Bureau of Investigation upon receiving fingerprints and other information provided by the employee or prospective employee. If the employee or prospective employee has been a resident of the State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State CIO and is not a public record under Chapter 132 of the General Statutes. (2015-241, s. 7A.2(b); 2015-268, ss. 2.12, 2.13.)

§ 143B-1337: Reserved for future codification purposes.

§ 143B-1338: Reserved for future codification purposes.

§ 143B-1339: Reserved for future codification purposes.

### Part 3. Information Technology Projects and Management.

#### § 143B-1340. Project management.

(a) Overall Management. – All information technology projects shall be managed through a standardized, fully documented process established and overseen by the State CIO. The State CIO shall be responsible for ensuring that participating agency information technology projects are completed on time, within budget, and meet all defined business requirements upon completion. For separate agency projects, the State CIO shall ensure that projects follow the Department's established process and shall monitor schedule, budget, and adherence to business

requirements. For all projects, the State CIO shall establish procedures to limit the need for change requests and shall report on this process to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division by January 1, 2016.

The State CIO shall also ensure that agency information technology project requirements are documented in biennial information technology plans. If an agency updates a biennial information technology plan to add a new project, the State CIO shall immediately report to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division on the reasons for the new requirement, the costs, and the sources of funding.

An agency that utilizes the system or software shall be designated as the sponsor for the information technology project or program and shall be responsible for overseeing the planning, development, implementation, and operation of the project or program. The Department and the assigned project managers shall advise and assist the designated agency for the duration of the project.

(b) Project Review and Approval. – The State CIO shall review, approve, and monitor all information technology projects for State agencies and shall be responsible for the efficient and timely management of all information technology projects for participating agencies. Project approval may be granted upon the State CIO's determination that (i) the project conforms to project management procedures and policies, (ii) the project does not duplicate a capability already existing in the State, (iii) the project conforms to procurement rules and policies, and (iv) sufficient funds are available.

(c) Project Implementation. – No State agency, unless expressly exempt within this Article, shall proceed with an information technology project until the State CIO approves the project. If a project is not approved, the State CIO shall specify in writing to the agency the grounds for denying the approval. The State CIO shall provide this information to the agency and the Office of State Budget and Management within five business days of the denial.

(d) Suspension of Approval/Cancellation of Projects. – The State CIO may suspend the approval of, or cancel, any information technology project that does not continue to meet the applicable quality assurance standards. The State CIO shall immediately suspend approval of, or cancel, any information technology project that is initiated without State CIO approval. Any project suspended or cancelled because of lack of State CIO approval cannot proceed until it completes all required project management documentation and meets criteria established by the State CIO for project approval, to include a statement from the State CIO that the project does not duplicate capabilities that already exist within the executive branch. If the State CIO suspends or cancels a project, the State CIO shall specify in writing to the agency the grounds for suspending or cancelling the approval. The State CIO shall provide this information to the agency within five business days of the suspension.

The Department shall report any suspension or cancellation immediately to the Office of the State Controller, the Office of State Budget and Management, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division. The Office of State Budget and Management shall not allow any additional expenditure of funds for a project that is no longer approved by the State CIO.

(e) General Quality Assurance. – Information technology projects authorized in accordance with this Article shall meet all project standards and requirements established under this Part.

(f) Performance Contracting. – All contracts between the State and a private party for information technology projects shall include provisions for vendor performance review and

accountability, contract suspension or termination, and termination of funding. The State CIO may require that these contract provisions include a performance bond, monetary penalties, or require other performance assurance measures for projects that are not completed within the specified time period or that involve costs in excess of those specified in the contract. The State CIO may utilize cost savings realized on government vendor partnerships as performance incentives for an information technology vendor.

(g) Notwithstanding the provisions of G.S. 114-2.3, any State agency developing and implementing an information technology project with a total cost of ownership in excess of five million dollars (\$5,000,000) may be required by the State CIO to engage the services of private counsel or subject matter experts with the appropriate information technology expertise. The private counsel or subject matter expert may review requests for proposals; review and provide advice and assistance during the evaluation of proposals and selection of any vendors; and review and negotiate contracts associated with the development, implementation, operation, and maintenance of the project. This requirement may also apply to information technology programs that are separated into individual projects if the total cost of ownership for the overall program exceeds five million dollars (\$5,000,000). (2015-241, s. 7A.2(b).)

#### **§ 143B-1341. Project management standards.**

(a) The State CIO shall establish standardized documentation requirements for agency projects to include requests for proposal and contracts. The State CIO shall establish standards for project managers and project management assistants. The State CIO shall develop performance measures for project reporting and shall make this reporting available through a publicly accessible Web site.

(b) **Participating Agency Responsibilities.** – The State CIO shall designate a Project Manager who shall select qualified personnel from the Department staff to participate in information technology project management, implementation, testing, and other activities for any information technology project. The Project Manager shall provide periodic reports to the project management assistant assigned to the project by the State CIO under subsection (d) of this section. The reports shall include information regarding the agency's business requirements, applicable laws and regulations, project costs, issues related to hardware, software, or training, projected and actual completion dates, and any other information related to the implementation of the information technology project.

(c) **Separate Agency Responsibilities.** – Each agency shall provide for one or more project managers who meet the applicable quality assurance standards for each information technology project that is subject to approval by the State CIO. Each project manager shall be subject to the review and approval of the State CIO. Each agency project manager shall provide periodic reports to the project management assistant assigned to the project by the State CIO under this subsection. The reports shall include information regarding project costs; issues related to hardware, software, or training; projected and actual completion dates; and any other information related to the implementation of the information technology project.

(d) **State CIO Responsibilities.** – The State CIO shall provide a project management assistant from the Department for any approved separate agency project, whether the project is undertaken in single or multiple phases or components. The State CIO may designate a project management assistant for any other information technology project.

The project management assistant shall advise the agency with the initial planning of a project, the content and design of any request for proposals, contract development, procurement,

and architectural and other technical reviews. The project management assistant shall also monitor progress in the development and implementation of the project and shall provide status reports to the agency and the State CIO, including recommendations regarding continued approval of the project.

The State CIO shall establish a clearly defined, standardized process for project management that includes time lines for completion of process requirements for both the Department and agencies. The State CIO shall also establish reporting requirements for information technology projects, both during the planning, development, and implementation process and following completion of the project. The State CIO shall continue to monitor system performance and financial aspects of each project after implementation. The State CIO shall also monitor any certification process required for State information technology projects and shall immediately report any issues associated with certification processes to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division. (2015-241, s. 7A.2(b).)

#### **§ 143B-1342. Dispute resolution.**

(a) Agency Request for Review. – In any instance where the State CIO has denied or suspended the approval of an information technology project, has cancelled the project, or has denied an agency's request for deviation, the affected State agency may request that the Governor review the State CIO's decision. The agency shall submit a written request for review to the Governor within 15 business days following the agency's receipt of the State CIO's written grounds for denial, suspension, or cancellation. The agency's request for review shall specify the grounds for its disagreement with the State CIO's determination. The agency shall include with its request for review a copy of the State CIO's written grounds for denial or suspension.

(b) Review Process. – The Governor shall review the information provided and may request additional information from either the agency or the State CIO. The Governor may affirm, reverse, or modify the decision of the State CIO or may remand the matter back to the State CIO for additional findings. Within 30 days after initial receipt of the agency's request for review, the Governor shall notify the agency and the State CIO of the decision in the matter. The notification shall be in writing and shall specify the grounds for the Governor's decision.

The Governor may reverse or modify a decision of the State CIO when the Governor finds the decision of the State CIO is unsupported by substantial evidence that the agency project fails to meet one or more standards of efficiency and quality of State government information technology as required under this Article. (2015-241, s. 7A.2(b).)

#### **§ 143B-1343. Standardization.**

The State CIO shall establish consistent standards for the purchase of agency hardware and software that reflect identified, documented agency needs. (2015-241, s. 7A.2(b).)

#### **§ 143B-1344. Legacy applications.**

Participating agency legacy applications shall be moved to the Department once a detailed plan is coordinated and in place for the successful transition of a specific application to the Department. The Department shall identify situations where multiple agencies are using legacy systems with similar capabilities and shall prepare plans to consolidate these systems. (2015-241, s. 7A.2(b); 2016-94, s. 7.4(c).)

§ 143B-1345: Reserved for future codification purposes.

§ 143B-1346: Reserved for future codification purposes.

§ 143B-1347: Reserved for future codification purposes.

§ 143B-1348: Reserved for future codification purposes.

§ 143B-1349: Reserved for future codification purposes.

#### Part 4. Information Technology Procurement.

##### § 143B-1350. Procurement of information technology.

(a) The State CIO is responsible for establishing policies and procedures for information technology procurement for State agencies.

Notwithstanding any other provision of law, the Department shall procure all information technology goods and services for participating agencies and shall approve information technology procurements for separate agencies. The State CIO may cancel or suspend any agency information technology procurement that occurs without State CIO approval.

(b) The Department shall review all procurements to ensure they meet current technology standards, are not duplicative, meet business objectives, are cost-effective, and are adequately funded. G.S. 143-135.9 shall apply to information technology procurements.

(c) The Department shall, subject to the provisions of this Part, do all of the following with respect to State information technology procurement:

- (1) Purchase or contract for all information technology for participating State agencies.
- (2) Approve all technology purchases for separate agencies.
- (3) Establish standardized, consistent processes, specifications, and standards that shall apply to all information technology to be purchased, licensed, or leased by State agencies and relating to information technology personal services contract requirements for State agencies, including, but not limited to, requiring convenience contracts to be rebid prior to termination without extensions.
- (4) Establish procedures to permit State agencies and local government entities to use the General Services Administration (GSA) Cooperative Purchasing Program to purchase information technology (i) awarded under GSA Supply Schedule 70 Information Technology and (ii) from contracts under the GSA's Consolidated Schedule containing information technology special item numbers.
- (5) Establish procedures to permit State agencies and local government entities to use other cooperative purchasing agreements.
- (6) Comply with the State government-wide technical architecture, as required by the State CIO.
- (7) Utilize the purchasing benchmarks established by the Secretary of Administration pursuant to G.S. 143-53.1.

- (8) Provide strategic sourcing resources and detailed, documented planning to compile and consolidate all estimates of information technology goods and services needed and required by State agencies.
- (9) Develop a process to provide a question and answer period for vendors prior to procurements.

(d) Each State agency shall furnish to the State CIO when requested, and on forms as prescribed, estimates of and budgets for all information technology goods and services needed and required by such department, institution, or agency for such periods in advance as may be designated by the State CIO. When requested, all State agencies shall provide to the State CIO on forms as prescribed, actual expenditures for all goods and services needed and required by the department, institution, or agency for such periods after the expenditures have been made as may be designated by the State CIO.

(e) Confidentiality. – Contract information compiled by the Department shall be made a matter of public record after the award of contract. Trade secrets, test data, similar proprietary information, and security information protected under G.S. 132-6.1(c) or other law shall remain confidential.

(f) Electronic Procurement. – The State CIO may authorize the use of the electronic procurement system established by G.S. 143-48.3, or other systems, to conduct reverse auctions and electronic bidding. For purposes of this Part, "reverse auction" means a real-time purchasing process in which vendors compete to provide goods or services at the lowest selling price in an open and interactive electronic environment. The vendor's price may be revealed during the reverse auction. The Department may contract with a third-party vendor to conduct the reverse auction. "Electronic bidding" means the electronic solicitation and receipt of offers to contract. Offers may be accepted and contracts may be entered by use of electronic bidding. All requirements relating to formal and competitive bids, including advertisement, seal, and signature, are satisfied when a procurement is conducted or a contract is entered in compliance with the reverse auction or electronic bidding requirements established by the Department.

(g) The State CIO shall establish efficient, responsive procedures for the procurement of information technology. The procedures may include aggregation of hardware purchases, the use of formal bid procedures, restrictions on supplemental staffing, enterprise software licensing, hosting, and multiyear maintenance agreements. The State CIO may require agencies to submit information technology procurement requests on a regularly occurring schedule each fiscal year in order to allow for bulk purchasing.

(h) All offers to contract, whether through competitive bidding or other procurement method, shall be subject to evaluation and selection by acceptance of the most advantageous offer to the State. Evaluation shall include best value, as the term is defined in G.S. 143-135.9(a)(1), compliance with information technology project management policies, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation.

(h1) All contracts subject to the provisions of this Part shall include a limitation on the contractor's liability to the State for damages. Except as otherwise provided in this subsection, the limitation of liability shall be for damages arising from any cause whatsoever, regardless of the form of action. The amount of liability shall be determined based on the nature of the goods or services covered by the contract; however, there shall be a presumptive limitation of no more than two times the value of the contract. Limitation of liability pursuant to this subsection shall

specifically include, but not be limited to, the contractor's liability for damages and any other losses relating to the loss of, unauthorized access to, or unauthorized disclosure of data.

The amount of liability for damages and any other losses relating to the loss of, unauthorized access to, or unauthorized disclosure of data may be raised to no more than three times the value of the contract if all of the following apply:

- (1) The State CIO completes a risk assessment prior to the bid solicitation or request for proposal.
- (2) The risk assessment determines that an increase in the liability amount is necessary to protect the State's best interests.
- (3) The bid solicitation or request for proposal indicates that increased liability will be required for the resulting contract.

The State CIO shall report annually to the Joint Legislative Commission on Governmental Operations and the Joint Legislative Oversight Committee on Information Technology no later than March 1 regarding the contracts containing liability amounts of more than two times the value of the contract.

Prior to entering into any contract subject to the provisions of this Part, the Department or the separate agency, as applicable, shall reasonably determine that the contractor possesses sufficient financial resources, either independently or through third-party sources, such as insurance, to satisfy the agreed upon limitation of liability. The limitation of liability required by this subsection shall not apply to liability of the contractor for intentional or willful misconduct, damage to tangible personal property, physical injuries to persons, or any notification costs resulting from compliance with G.S. 132-1.10(c1). Nothing in this subsection (i) limits the contractor's liability directly to third parties or (ii) affects the rights and obligations related to contribution among joint tortfeasors established by Chapter 1B of the General Statutes and other applicable law.

(i) Exceptions. – In addition to permitted waivers of competition, the requirements of competitive bidding shall not apply to information technology contracts and procurements:

- (1) In cases of pressing need or emergency arising from a security incident.
- (2) In the use of master licensing or purchasing agreements governing the Department's acquisition of proprietary intellectual property.

Any exceptions shall immediately be reported to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.

(j) Information Technology Innovation Center. – The Department may operate a State Information Technology Innovation Center (iCenter) to develop and demonstrate technology solutions with potential benefit to the State and its citizens. The iCenter may facilitate the piloting of potential solutions to State technology requirements. In operating the iCenter, the State CIO shall ensure that all State laws, rules, and policies are followed.

Vendor participation in the iCenter shall not be construed to (i) create any type of preferred status for vendors or (ii) abrogate the requirement that agency and statewide requirements for information technology support, including those of the Department, are awarded based on a competitive process that follows information technology procurement guidelines.

(k) No contract subject to the provisions of this Part may be entered into unless the contractor and the contractor's subcontractors comply with the requirements of Article 2 of Chapter 64 of the General Statutes. (2015-241, s. 7A.2(b); 2015-268, ss. 2.14, 2.20; 2016-85, s. 1.)

**§ 143B-1351. Restriction on State agency contractual authority with regard to information technology.**

(a) All State agencies covered by this Article shall use contracts for information technology to include enterprise licensing agreements and convenience contracts established by the Department. The State CIO shall consult the agency heads prior to the initiation of any enterprise project or contract. Notwithstanding any other statute, the authority of State agencies to procure or obtain information technology shall be subject to compliance with the provisions of this Part.

(b) Notwithstanding any other provision of law, local governmental entities may use 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. Local governmental entities are not required to comply with otherwise applicable competitive bidding requirements when using contracts established by the Department.

(c) Any other State entities exempt from Part 3 or Part 5 of this Article may also use 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. (2015-241, s. 7A.2(b).)

**§ 143B-1352. Unauthorized use of public purchase or contract procedures for private benefit prohibited.**

(a) It is unlawful for any person, by the use of the powers, policies, or procedures described in this Part or established hereunder, to purchase, attempt to purchase, procure, or attempt to procure any property or services for private use or benefit.

(b) This prohibition shall not apply if:

(1) The State agency through which the property or services are procured had theretofore established policies and procedures permitting such purchases or procurement by a class or classes of persons in order to provide for the mutual benefit of such persons and the department, institution, or agency involved or the public benefit or convenience; and

(2) Such policies and procedures, including any reimbursement policies, are complied with by the person permitted thereunder to use the purchasing or procurement procedures described in this Part or established thereunder.

(c) Any violation of this section is a Class 1 misdemeanor.

(d) Any employee or official of the State who violates this Part shall be liable to the State to repay any amount expended in violation of this Part, together with any court costs. (2015-241, s. 7A.2(b).)

**§ 143B-1353. Financial interest of officers in sources of supply; acceptance of bribes.**

Neither the State CIO, any deputy State CIO, or any other policy-making or managerially exempt personnel shall be financially interested, or have any personal beneficial interest, either directly or indirectly, in the purchase of, or contract for, any information technology, nor in any firm, corporation, partnership, or association furnishing any information technology to the State government or any of its departments, institutions, or agencies, nor shall any of these persons or any other Department employee accept or receive, directly or indirectly, from any person, firm, or corporation to whom any contract may be awarded, by rebate, gifts, or otherwise, any money or anything of value whatsoever, or any promise, obligation, or contract for future reward or

compensation. Violation of this section is a Class F felony, and any person found guilty of a violation of this section shall, upon conviction, be removed from State office or employment. (2015-241, s. 7A.2(b).)

**§ 143B-1354. Certification that information technology bid submitted without collusion.**

The State CIO shall require bidders to certify that each bid on information technology contracts overseen by the Department is submitted competitively and without collusion. False certification is a Class I felony. (2015-241, s. 7A.2(b).)

**§ 143B-1355. Award review.**

(a) When the dollar value of a contract for the procurement of information technology equipment, materials, and supplies exceeds the benchmark established by subdivision (1) of subsection (c) of this section, an award recommendation shall be submitted to the State CIO for approval or other action. The State CIO shall promptly notify the agency or institution making the recommendation, or for which the purchase is to be made, of the action taken.

(b) Prior to submission for review pursuant to this section for any contract for information technology being acquired for the benefit of an agency authorized to deviate from this Article pursuant to G.S. 143B-1320(c), the State CIO shall review and approve the procurement to ensure compliance with the established processes, specifications, and standards applicable to all information technology purchased, licensed, or leased in State government, including established procurement processes, and compliance with the State government-wide technical architecture and standards established by the State CIO.

(c) The State CIO shall provide a report of all contract awards approved through the Statewide Procurement Office as indicated below. The report shall include the amount of the award, the contract term, the award recipient, the using agency, and a short description of the nature of the award, as follows:

- (1) For contract awards greater than twenty-five thousand dollars (\$25,000), to the cochairs of the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division as requested.
- (2) For all contract awards outside the established purchasing system, to the Department of Administration, Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division on March 1 and September 1 of each year. (2015-241, s. 7A.2(b); 2016-94, s. 7.4(a).)

**§ 143B-1356. Multiyear contracts; Attorney General assistance.**

(a) Notwithstanding the cash management provisions of G.S. 147-86.11, the Department may procure information technology goods and services for periods up to a total of three years where the terms of the procurement contracts require payment of all or a portion of the contract price at the beginning of the contract agreement. All of the following conditions shall be met before payment for these agreements may be disbursed:

- (1) Any advance payment can be accomplished within the IT Internal Service Fund budget.
- (2) The State Controller receives conclusive evidence that the proposed agreement would be more cost-effective than a multiyear agreement that complies with G.S. 147-86.11.

- (3) The procurement complies in all other aspects with applicable statutes and rules.
- (4) The proposed agreement contains contract terms that protect the financial interest of the State against contractor nonperformance or insolvency through the creation of escrow accounts for funds, source codes, or both, or by any other reasonable means that have legally binding effect.

The Office of State Budget and Management shall ensure the savings from any authorized agreement shall be included in the IT Internal Service Fund rate calculations before approving annual proposed rates. Any savings resulting from the agreements shall be returned to agencies included in the contract in the form of reduced rates.

(b) At the request of the State CIO, the Attorney General shall provide legal advice and services necessary to implement this Article. (2015-241, s. 7A.2(b).)

**§ 143B-1357. Purchase of certain computer equipment and televisions by State agencies and governmental entities prohibited.**

(a) No State agency, local political subdivision of the State, or other public body shall purchase computer equipment or televisions, as defined in G.S. 130A-309.131, or enter into a contract with any manufacturer that the State CIO determines is not in compliance with the requirements of G.S. 130A-309.134 or G.S. 130A-309.135 as determined from the list provided by the Department of Environmental Quality pursuant to G.S. 130A-309.138. The State CIO shall issue written findings upon a determination of noncompliance. A determination of noncompliance by the State CIO is reviewable under Article 3 of Chapter 150B of the General Statutes.

(b) The Department shall make the list available to local political subdivisions of the State and other public bodies. A manufacturer that is not in compliance with the requirements of G.S. 130A-309.134 or G.S. 130A-309.135 shall not sell or offer for sale computer equipment or televisions to the State, a local political subdivision of the State, or other public body. (2015-241, ss. 7A.2(b), 14.30(c).)

**§ 143B-1358. Refurbished computer equipment purchasing program.**

(a) The Department of Information Technology and the Department of Administration, with the administrative support of the Information Technology Strategic Sourcing Office, shall offer State and local governmental entities the option of purchasing refurbished computer equipment from registered computer equipment refurbishers whenever most appropriate to meet the needs of State and local governmental entities.

(b) State and local governmental entities shall document savings resulting from the purchase of the refurbished computer equipment, including, but not limited to, the initial acquisition cost as well as operations and maintenance costs. These savings shall be reported quarterly to the Department of Information Technology.

(c) The Information Technology Strategic Sourcing Office shall administer the refurbished computer equipment program by establishing a competitive purchasing process to support this initiative that meets all State information technology procurement laws and procedures and ensures that agencies receive the best value.

(d) Participating computer equipment refurbishers must meet all procurement requirements established by the Department of Information Technology and the Department of Administration. (2015-241, s. 7A.2(b).)

**§ 143B-1359. Configuration and specification requirements same as for new computers.**

Refurbished computer equipment purchased under this act must conform to the same standards as the State may establish as to the configuration and specification requirements for the purchase of new computers. (2015-241, s. 7A.2(b).)

**§ 143B-1360. Data on reliability and other issues; report.**

The Department of Information Technology shall maintain data on equipment reliability, potential cost savings, and any issues associated with the refurbished computer equipment initiative and shall report the results of the initiative to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division by March 1, 2016, and then annually thereafter. (2015-241, s. 7A.2(b); 2016-94, s. 7.4(b).)

**§ 143B-1361. Information technology procurement policy; reporting requirements.**

(a) Policy. – In order to further the policy of the State to encourage and promote the use of small, minority, physically handicapped, and women contractors in State purchasing of goods and services, all State agencies shall cooperate with the Department in efforts to encourage the use of small, minority, physically handicapped, and women contractors in achieving the purposes of this Article, which is to provide for the effective and economical acquisition, management, and disposition of information technology.

(b) Bids. – A vendor submitting a bid shall disclose in a statement, provided contemporaneously with the bid, where services will be performed under the contract sought, including any subcontracts and whether any services under that contract, including any subcontracts, are anticipated to be performed outside the United States. Nothing in this section is intended to contravene any existing treaty, law, agreement, or regulation of the United States. The State CIO shall retain the statements required by this subsection regardless of the State entity that awards the contract and shall report annually to the Secretary of Administration on the number of contracts which are anticipated to be performed outside the United States.

(c) Reporting. – Every State agency that makes a direct purchase of information technology using the services of the Department shall report directly to the Department of Administration all information required by G.S. 143-48(b).

(d) Data from Department of Administration. – The Department of Administration shall collect and compile the data described in this section and report it annually to the Department of Information Technology, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division. (2015-241, s. 7A.2(b).)

**§ 143B-1362. Personal services contracts subject to Article.**

(a) Requirement. – Notwithstanding any other provision of law, information technology personal services contracts for executive branch agencies shall be subject to the same requirements and procedures as information technology service contracts, except as provided in this section.

(b) Certain Approvals Required. – Notwithstanding any provision of law to the contrary, no information technology personal services contract, nor any contract that provides personnel to perform information technology functions regardless of the cost of the contract, may be established or renewed without written approval from the Department of Information Technology and the Office of State Budget and Management. To facilitate compliance with this

requirement, the Department of Information Technology shall develop and document the following:

- (1) Standards for determining whether it is more appropriate for an agency to hire an employee or use the services of a vendor.
- (2) A process to monitor all State agency information technology personal services contracts, as well as any other State contracts providing personnel to perform information technology functions.
- (3) A process for obtaining approval of contractor positions.

(c) **Creation of State Positions in Certain Cases.** – The Department of Information Technology shall review current information technology personal services contracts on an ongoing basis and determine if each contractor is performing a function that could more appropriately be performed by a State employee. Where the determination is made that a State employee should be performing the function, the Department of Information Technology shall work with the impacted agency and the Office of State Human Resources to identify or create the position.

(d) **Compliance Audits Required.** – The Department of Information Technology shall conduct periodic audits of State agencies that are subject to this Article to determine the degree to which those agencies are complying with the rules and procedures that govern information technology personal services contracts.

(e) **Reporting Required.** – The Department of Information Technology shall report biennially to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division on all of the following:

- (1) Its progress toward standardizing information technology personal services contracts.
- (2) The number of information technology service contractors in each State agency, the cost for each, and the comparable cost, including benefits, of a State employee serving in that capacity rather than a contractor.
- (3) The results of the compliance audits conducted pursuant to subsection (d) of this section.

(f) **Information Technology Personal Services Contract Defined.** – For purposes of this section, the term "personal services contract" means a contract for services provided by a professional individual as an independent contractor on a temporary or occasional basis.

(g) **Rules Required.** – The Department of Information Technology shall adopt rules consistent with this section. (2015-241, s. 26.2(b).)

§ 143B-1363: Reserved for future codification purposes.

§ 143B-1364: Reserved for future codification purposes.

#### Part 5. Data Centers.

##### § 143B-1365. Data centers.

(a) The State CIO shall create an inventory of data center operations in the executive branch and shall develop and implement a detailed, written plan for consolidation of agency data centers in the most efficient manner possible. By May 1, 2016, the State CIO shall present a report on the data center consolidation plan to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.

(b) State agencies shall use the State infrastructure to host their projects, services, data, and applications. The State Chief Information Officer may grant an exception if the State agency can demonstrate any of the following:

- (1) Using an outside contractor would be more cost-effective for the State.
- (2) The Department does not have the technical capabilities required to host the application.
- (3) Valid security requirements preclude the use of State infrastructure, and a vendor can provide a more secure environment. (2015-241, s. 7A.2(b).)

§ 143B-1366: Reserved for future codification purposes.

§ 143B-1367: Reserved for future codification purposes.

§ 143B-1368: Reserved for future codification purposes.

§ 143B-1369: Reserved for future codification purposes.

#### Part 6. Communications and Portal Services.

##### § 143B-1370. **Communications services.**

(a) The State CIO shall exercise authority for telecommunications and other communications included in information technology relating to the internal management and operations of State agencies. In discharging that responsibility, the State CIO shall do the following:

- (1) Develop standards for a State network.
- (2) Develop a detailed plan for the standardization and operation of State communications networks and services.
- (3) Establish an inventory of communications systems in use within the State and ensure that the State is using the most efficient and cost-effective means possible.
- (4) Identify shortfalls in current network operations and develop a strategy to mitigate the identified shortfalls.
- (5) Provide for the establishment, management, and operation, through either State ownership, by contract, or through commercial leasing, of the following systems and services as they affect the internal management and operation of State agencies:
  - a. Central telephone systems and telephone networks, including Voice over Internet Protocol and Commercial Mobile Radio Systems.
  - b. Satellite services.
  - c. Closed-circuit TV systems.
  - d. Two-way radio systems.
  - e. Microwave systems.
  - f. Related systems based on telecommunication technologies.
  - g. The "State Network," managed by the Department, which means any connectivity designed for the purpose of providing Internet Protocol transport of information for State agencies.
  - h. Broadband.

- (6) Coordinate the development of cost-sharing systems for respective user agencies for their proportionate parts of the cost of maintenance and operation of the systems and services listed in subdivision (5) of this subsection.
- (7) Assist in the development of coordinated telecommunications services or systems within and among all State agencies and recommend, where appropriate, cooperative utilization of telecommunication facilities by aggregating users.
- (8) Perform traffic analysis and engineering for all telecommunications services and systems listed in subdivision (5) of this subsection.
- (9) Establish telecommunications specifications and designs so as to promote and support compatibility of the systems within State agencies.
- (10) Provide a periodic inventory of telecommunications costs, facilities, systems, and personnel within State agencies.
- (11) Promote, coordinate, and assist in the design and engineering of emergency telecommunications systems, including, but not limited to, the 911 emergency telephone number program, Emergency Medical Services, and other emergency telecommunications services.
- (12) Perform frequency coordination and management for State agencies and local governments, including all public safety radio service frequencies, in accordance with the rules and regulations of the Federal Communications Commission or any successor federal agency.
- (13) Advise all State agencies on telecommunications management planning and related matters and provide through the State Personnel Training Center or the Department training to users within State agencies in telecommunications technology and systems.
- (14) Assist and coordinate the development of policies and long-range plans, consistent with the protection of citizens' rights to privacy and access to information, for the acquisition and use of telecommunications systems, and base such policies and plans on current information about State telecommunications activities in relation to the full range of emerging technologies.

(b) The provisions of this section shall not apply to the Judicial Information System in the Judicial Department. (2015-241, s. 7A.2(b).)

**§ 143B-1371. Communications services for local governmental entities and other entities.**

(a) The State CIO shall provide cities, counties, and other local governmental entities with access to communications systems or services established by the Department under this Part for State agencies. Access shall be provided on the same cost basis that applies to State agencies.

(b) The State CIO shall establish broadband communications services and permit, in addition to State agencies, cities, counties, and other local government entities, the following organizations and entities to share on a not-for-profit basis:

- (1) Nonprofit educational institutions as defined in G.S. 116-280.
- (2) MCNC and research affiliates of MCNC for use only in connection with research activities sponsored or funded, in whole or in part, by MCNC, if such research activities relate to health care or education in North Carolina.

- (3) Agencies of the United States government operating in North Carolina for use only in connection with activities that relate to health care, education, or FirstNet in North Carolina.
- (4) Hospitals, clinics, and other health care facilities for use only in connection with activities that relate to health care, education, or FirstNet in North Carolina.

(c) Any communications or broadband telecommunications services provided pursuant to this section shall not be provided in a manner that would cause the State or the Department to be classified as a public utility as that term is defined in G.S. 62-3(23)a.6., nor as a retailer as that term is defined in G.S. 105-164.3. Nor shall the State or the Department engage in any activities that may cause those entities to be classified as a common carrier as that term is defined in the Communications Act of 1934, 47 U.S.C. § 153(11). Provided further, authority to share communications services with the non-State agencies set forth in subdivisions (1) through (4) of subsection (b) of this section shall terminate not later than one year from the effective date of a tariff for such service or federal law that preempts this section. (2015-241, s. 7A.2(b).)

**§ 143B-1372. Statewide electronic web presence; annual report.**

(a) The Department shall plan, develop, implement, and operate a statewide electronic web presence, to include mobile, in order to (i) increase the convenience of members of the public in conducting online transactions with, and obtaining information from, State government and (ii) facilitate the public's interactions and communications with government agencies. The State CIO shall have approval authority over all agency Web site funding, to include any agency contract decisions. Participating agency Web site and content development staff shall be transferred to the Department in accordance with the schedule for their agency.

(b) Beginning January 1, 2016, and then annually thereafter, the State CIO shall report to the General Assembly and to the Fiscal Research Division on the following information:

- (1) Services currently provided and associated transaction volumes or other relevant indicators of utilization by user type.
- (2) New services added during the previous year.
- (3) Services added that are currently available in other states.
- (4) The total amount collected for each service.
- (5) The total amount remitted to the State for each service.
- (6) The total amount remitted to the vendor for each service.
- (7) Any other use of State data by the vendor and the total amount of revenue collected per each use and in total.
- (8) Customer satisfaction with each service.
- (9) Any other issues associated with the provision of each service. (2015-241, s. 7A.2(b); 2015-268, s. 2.16.)

**§ 143B-1373:** Reserved for future codification purposes.

**§ 143B-1374:** Reserved for future codification purposes.

Part 7. Security of Information Technology.

**§ 143B-1375. Security.**

Confidentiality. – No data of a confidential nature, as defined in the General Statutes or federal law, may be entered into or processed through any information technology system or network established under this Article until safeguards for the data's security satisfactory to the State CIO have been designed and installed and are fully operational. This section does not affect the provisions of G.S. 147-64.6 or G.S. 147-64.7. (2015-241, s. 7A.2(b).)

**§ 143B-1376. Statewide security standards.**

(a) The State CIO shall be responsible for the security of all State information technology systems and associated data. The State CIO shall manage all executive branch information technology security and shall establish a statewide standard for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. The State CIO shall review and revise the security standards annually. As part of this function, the State CIO shall review periodically existing security standards and practices in place among the various State agencies to determine whether those standards and practices meet statewide security and encryption requirements. The State CIO may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to security standards adopted under this Article.

(b) The State CIO shall establish standards for the management and safeguarding of all State data held by State agencies and private entities and shall develop and implement a process to monitor and ensure adherence to the established standards. The State CIO shall establish and enforce standards for the protection of State data. The State CIO shall develop and maintain an inventory of where State data is stored. For data maintained by non-State entities, the State CIO shall document the reasons for the use of the non-State entity and certify, in writing, that the use of the non-State entity is the best course of action. The State CIO shall ensure that State data held by non-State entities is properly protected and is held in facilities that meet State security standards. By October 1 each year, the State CIO shall certify in writing that data held in non-State facilities is being maintained in accordance with State information technology security standards and shall provide a copy of this certification to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.

(c) Before a State agency can contract for the storage, maintenance, or use of State data by a private vendor, the agency shall obtain the approval of the State CIO. (2015-241, s. 7A.2(b).)

**§ 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.)

#### **§ 143B-1378. Assessment of agency compliance with security standards.**

At a minimum, the State CIO shall annually assess the ability of each State agency, and each agency's contracted vendors, to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security. The assessment of a State agency shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each State agency shall submit information required by the State CIO for purposes of this assessment. The State CIO shall include the information obtained from the assessment in the State Information Technology Plan. (2015-241, s. 7A.2(b).)

#### **§ 143B-1379. State agency cooperation; liaisons.**

(a) The head of each principal department and Council of State agency shall cooperate with the State CIO in the discharge of the State CIO's duties by providing the following information to the Department:

- (1) The full details of the State agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation.
- (2) Comprehensive information concerning the information technology security employed to protect the agency's information technology.
- (3) A forecast of the parameters of the agency's projected future information technology security needs and capabilities.
- (4) Designating an agency liaison in the information technology area to coordinate with the State CIO. The liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving

fingerprints from the liaison. If the liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State CIO and the head of the agency. In addition, all personnel in the Office of the State Auditor who are responsible for information technology security reviews shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor. For designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background reports shall be provided to the State Auditor. Criminal histories provided pursuant to this subdivision are not public records under Chapter 132 of the General Statutes.

(b) The information provided by State agencies to the State CIO under this section is protected from public disclosure pursuant to G.S. 132-6.1(c). (2015-241, s. 7A.2(b).)

§ 143B-1380: Reserved for future codification purposes.

§ 143B-1381: Reserved for future codification purposes.

§ 143B-1382: Reserved for future codification purposes.

§ 143B-1383: Reserved for future codification purposes.

§ 143B-1384: Reserved for future codification purposes.

#### Part 8. Government Data Analytics Center.

#### § 143B-1385. Government Data Analytics Center.

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

- (1) Business intelligence. – The process of collecting, organizing, sharing, and analyzing data through integrated data management, reporting, visualization, and advanced analytics to discover patterns and other useful information that will allow policymakers and State officials to make more informed decisions. Business intelligence also includes both of the following:
  - a. Broad master data management capabilities such as data integration, data quality and enrichment, data governance, and master data management to collect, reference, and categorize information from multiple sources.
  - b. Self-service query and reporting capabilities to provide timely, relevant, and actionable information to business users delivered through a variety of interfaces, devices, or applications based on their specific roles and responsibilities.
- (2) Data analytics. – Data analysis, including the ability to use the data for assessment and extraction of policy relevant information.

- (3) Enterprise-level data analytics. – Standard analytics capabilities and services leveraging data throughout all State agencies, departments, and institutions.
  - (4) Operationalize. – The implementation process whereby a State agency, department, or institution integrates analytical output into current business processes and systems in order to improve operational efficiency and decision making.
- (b) GDAC. – The Government Data Analytics Center is established as a unit of the Department.
- (1) Purpose. – The purpose of the GDAC is to utilize public-private partnerships as part of a statewide data integration and data-sharing initiative and to identify data integration and business intelligence opportunities that will generate greater efficiencies in, and improved service delivery by, State agencies, departments, and institutions. The intent is not to replace transactional systems but to leverage the data from those systems for enterprise-level State business intelligence. The GDAC shall continue the work, purpose, and resources of previous data integration efforts and shall otherwise advise and assist the State CIO in the management of the initiative. The State CIO shall make any organizational changes necessary to maximize the effectiveness and efficiency of the GDAC.
  - (2) Public-private partnerships. – The State CIO shall continue to utilize public-private partnerships and existing data integration and analytics contracts and licenses as appropriate to continue the implementation of the initiative. Private entities that partner with the State shall make appropriate contributions of funds or resources, including, but not limited to, knowledge transfer and education activities, software licensing, hardware and technical infrastructure resources, personnel resources, and such other appropriate resources as agreed upon by the parties.
  - (3) Powers and duties. – The State CIO shall, through the GDAC, do all of the following:
    - a. Manage and coordinate enterprise data integration efforts, including:
      - 1. The deployment, support, technology improvements, and expansion of the Criminal Justice Law Enforcement Automated Data System (CJLEADS) and related intelligence-based case management systems.
      - 2. The deployment, support, technology improvements, and expansion of the North Carolina Financial Accountability and Compliance Technology System (NCFACS) in order to collect data that will create efficiencies and detect fraud, waste, and abuse across State government.
      - 3. The development, deployment, support, technology improvements, and expansion of the GDAC Enterprise Solutions.
      - 4. Individual-level student data and workforce data from all levels of education and the State workforce.
      - 5. The integration of all available financial data to support more comprehensive State budget and financial analyses.

6. Other capabilities as developed by the GDAC.
  - b. Identify technologies currently used in North Carolina that have the capability to support the initiative.
  - c. Identify other technologies, especially those with unique capabilities that are complementary to existing GDAC analytic solutions that could support the State's business intelligence effort.
  - d. Compare capabilities and costs across State agencies.
  - e. Ensure implementation is properly supported across State agencies.
  - f. Ensure that data integration and sharing is performed in a manner that preserves data privacy and security in transferring, storing, and accessing data, as appropriate.
  - g. Immediately seek any waivers and enter into any written agreements that may be required by State or federal law to effectuate data sharing and to carry out the purposes of this section.
  - h. Coordinate data requirements and usage for State business intelligence applications in a manner that (i) limits impacts on participating State agencies as those agencies provide data and business knowledge expertise, (ii) assists in defining business rules so the data can be properly used, and (iii) ensures participating State agencies operationalize analytics and report outcomes.
  - i. Recommend the most cost-effective and reliable long-term hosting solution for enterprise-level State business intelligence as well as data integration, notwithstanding any other provision of State law or regulation.
  - j. Utilize a common approach that establishes standards for business intelligence initiatives for all State agencies and prevents the development of projects that do not meet the established standards.
  - k. Create efficiencies in State government by ensuring that State agencies use the GDAC for agency business intelligence requirements.
  - l. Assist State agencies in developing requirements for the integration or creation of an interface with State agencies' workflow processes and transactional systems to operationalize GDAC analytic solutions.
  - m. Establish clear metrics and definitions with participating State agencies for reporting outcomes for each GDAC project.
  - n. Evaluate State agency business intelligence projects to determine the feasibility of integrating analytics and reporting with the GDAC and to determine what GDAC services may support the projects.
- (4) Application to State government. – The initiative shall include all State agencies, departments, and institutions, including The University of North Carolina, as follows:
- a. All State agency business intelligence requirements, including any planning or development efforts associated with creating business intelligence capability, as well as any master data management efforts, shall be implemented through the GDAC.
  - b. The Chief Justice of the North Carolina Supreme Court and the Legislative Services Commission each shall designate an officer or

agency to advise and assist the State CIO with respect to implementation of the initiative in their respective branches of government. The judicial and legislative branches shall fully cooperate in the initiative mandated by this section in the same manner as is required of State agencies.

- (5) Project management. – The State CIO and State agencies, with the assistance of the Office of State Budget and Management, shall identify potential funding sources for expansion of existing projects or development of new projects. No GDAC project shall be initiated, extended, or expanded:
  - a. Without the specific approval of the General Assembly, unless the project can be implemented within funds appropriated for GDAC projects.
  - b. Without prior consultation to the Joint Legislative Commission on Governmental Operations and a report to the Joint Legislative Oversight Committee on Information Technology if the project can be implemented within funds appropriated for GDAC projects.
- (c) Data Sharing. –
  - (1) General duties of all State agencies. – Except as limited or prohibited by federal law, the head of each State agency, department, and institution shall do all of the following:
    - a. Grant the State CIO and the GDAC access to all information required to develop and support State business intelligence applications pursuant to this section. The State CIO and the GDAC shall take all necessary actions and precautions, including training, certifications, background checks, and governance policy and procedure, to ensure the security, integrity, and privacy of the data in accordance with State and federal law and as may be required by contract.
    - b. Provide complete information on the State agency's information technology, operational, and security requirements.
    - c. Provide information on all of the State agency's information technology activities relevant to the State business intelligence effort.
    - d. Forecast the State agency's projected future business intelligence information technology needs and capabilities.
    - e. Ensure that the State agency's future information technology initiatives coordinate efforts with the GDAC to include planning and development of data interfaces to incorporate data into the initiative and to ensure the ability to leverage analytics capabilities.
    - f. Provide technical and business resources to participate in the initiative by providing, upon request and in a timely and responsive manner, complete and accurate data, business rules and policies, and support.
    - g. Identify potential resources for deploying business intelligence in their respective State agencies and as part of the enterprise-level effort.
    - h. Immediately seek any waivers and enter into any written agreements that may be required by State or federal law to effectuate data sharing and to carry out the purposes of this section, as appropriate.

- (2) Specific agency requirements. – The following agency-specific requirements are designed to illustrate but not limit the type and extent of data and information required to be released under subdivision (1) of this subsection:
- a. The North Carolina Industrial Commission shall release to the GDAC, or otherwise provide electronic access to, all data requested by the GDAC relating to workers' compensation insurance coverage, claims, appeals, compliance, and enforcement under Chapter 97 of the General Statutes.
  - b. The North Carolina Rate Bureau (Bureau) shall release to the GDAC, or otherwise provide electronic access to, all data requested by the GDAC relating to workers' compensation insurance coverage, claims, business ratings, and premiums under Chapter 58 of the General Statutes. The Bureau shall be immune from civil liability for releasing information pursuant to this subsection, even if the information is erroneous, provided the Bureau acted in good faith and without malicious or willful intent to harm in releasing the information.
  - c. The Department of Commerce, Division of Employment Security (DES), shall release to the GDAC, or otherwise provide access to, all data requested by the GDAC relating to unemployment insurance coverage, claims, and business reporting under Chapter 96 of the General Statutes.
  - d. The Department of Labor shall release to the GDAC, or otherwise provide access to, all data requested by the GDAC relating to safety inspections, wage and hour complaints, and enforcement activities under Chapter 95 of the General Statutes.
  - e. The Department of Revenue shall release to the GDAC, or otherwise provide access to, all data requested by the GDAC relating to the registration and address information of active businesses, business tax reporting, and aggregate federal tax Form 1099 data for comparison with information from DES, the Rate Bureau, and the Department of the Secretary of State for the evaluation of business reporting. Additionally, the Department of Revenue shall furnish to the GDAC, upon request, other tax information, provided that the information furnished does not impair or violate any information-sharing agreements between the Department and the United States Internal Revenue Service. Notwithstanding any other provision of law, a determination of whether furnishing the information requested by the GDAC would impair or violate any information-sharing agreements between the Department of Revenue and the United States Internal Revenue Service shall be within the sole discretion of the State Chief Information Officer. The Department of Revenue and the Office of the State CIO shall work jointly to assure that the evaluation of tax information pursuant to this sub-subdivision is performed in accordance with applicable federal law.
  - f. The North Carolina Department of Health and Human Services, pursuant to this Part, shall share (i) claims data from NTRACKS and

the accompanying claims data warehouse and (ii) encounter data with the GDAC in order to leverage existing public-private partnerships and subject matter expertise that can assist in providing outcome-based analysis of services and programs as well as population health analytics of the Medicaid and LME/MCO patient population.

- (3) All information shared with the GDAC and the State CIO under this subsection is protected from release and disclosure in the same manner as any other information is protected under this subsection.
- (d) Provisions on Privacy and Confidentiality of Information.
- (1) Status with respect to certain information. – The State CIO and the GDAC shall be deemed to be all of the following for the purposes of this section:
    - a. A criminal justice agency (CJA), as defined under Criminal Justice Information Services (CJIS) Security Policy. The State CJIS Systems Agency (CSA) shall ensure that CJLEADS receives access to federal criminal information deemed to be essential in managing CJLEADS to support criminal justice professionals.
    - b. With respect to health information covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and to the extent allowed by federal law:
      1. A business associate with access to protected health information acting on behalf of the State's covered entities in support of data integration, analysis, and business intelligence.
      2. Authorized to access and view individually identifiable health information, provided that the access is essential to the enterprise fraud, waste, and improper payment detection program or required for future initiatives having specific definable need for such data.
    - c. Authorized to access all State and federal data, including revenue and labor information, deemed to be essential to the enterprise fraud, waste, and improper payment detection program or future initiatives having specific definable need for the data.
    - d. Authorized to develop agreements with the federal government to access data deemed to be essential to the enterprise fraud, waste, and improper payment detection program or future initiatives having specific definable need for such data.
  - (2) Release of information. – The following limitations apply to (i) the release of information compiled as part of the initiative, (ii) data from State agencies that is incorporated into the initiative, and (iii) data released as part of the implementation of the initiative:
    - a. Information compiled as part of the initiative. – Notwithstanding the provisions of Chapter 132 of the General Statutes, information compiled by the State CIO and the GDAC related to the initiative may be released as a public record only if the State CIO, in that officer's sole discretion, finds that the release of information is in the best interest of the general public and is not in violation of law or contract.

- b. Data from State agencies. – Any data that is not classified as a public record under G.S. 132-1 shall not be deemed a public record when incorporated into the data resources comprising the initiative. To maintain confidentiality requirements attached to the information provided to the State CIO and the GDAC, each source agency providing data shall be the sole custodian of the data for the purpose of any request for inspection or copies of the data under Chapter 132 of the General Statutes.
- c. Data released as part of implementation. – Information released to persons engaged in implementing the State's business intelligence strategy under this section that is used for purposes other than official State business is not a public record pursuant to Chapter 132 of the General Statutes.
- d. Data from North Carolina Rate Bureau. – Notwithstanding any other provision of this section, any data released by or obtained from the North Carolina Rate Bureau under this initiative relating to workers' compensation insurance claims, business ratings, or premiums are not public records, and public disclosure of such data, in whole or in part, by the GDAC or State CIO, or by any State agency, is prohibited.

(e) Funding. – The Department of Information Technology, with the support of the Office of State Budget and Management, shall identify and make all efforts to secure any matching funds or other resources to assist in funding the GDAC. Savings resulting from the cancellation of projects, software, and licensing, as well as any other savings from the utilization of the GDAC, shall be returned to the General Fund and shall remain unexpended and unencumbered until appropriated by the General Assembly in a subsequent fiscal year. It is the intent of the General Assembly that expansion of the GDAC in subsequent fiscal years be funded with these savings and that the General Assembly appropriate funds for projects in accordance with the priorities identified by the State CIO.

(f) Reporting. – The State CIO shall:

- (1) On or before March 1 of each year, submit and present a report on the activities described in this section to the Chairs of the House of Representatives Appropriations and Senate Base Budget/Appropriations Committees, to the Joint Legislative Oversight Committee on Information Technology, and to the Fiscal Research Division of the General Assembly. The report shall include the following:
  - a. A description of project funding and expenditures, cost savings, cost avoidance, efficiency gains, process improvements, and major accomplishments. Cost savings and cost avoidance shall include immediate monetary impacts as well as ongoing projections.
  - b. A description of the contribution of funds or resources by those private entities which are participating in public-private partnerships under this section, including, but not limited to, knowledge transfer and education activities, software licensing, hardware and technical infrastructure resources, personnel resources, and such other resources as agreed upon by the State and the private entity.
- (2) Report the following information upon its occurrence or as requested:

- a. Any failure of a State agency to provide information requested pursuant to this section. The failure shall be reported to the Joint Legislative Oversight Committee on Information Technology and to the Chairs of the House of Representatives Appropriations and Senate Base Budget/Appropriations Committees.
- b. Any additional information to the Joint Legislative Commission on Governmental Operations and the Joint Legislative Oversight Committee on Information Technology that is requested by those entities. (2013-360, s. 7.10(d); 2013-363, s. 2.4(a); 2014-100, s. 7.6(a); 2014-115, s. 56.8(a); 2015-241, s. 7A.2(c).)

§ 143B-1386: Reserved for future codification purposes.

§ 143B-1387: Reserved for future codification purposes.

§ 143B-1388: Reserved for future codification purposes.

§ 143B-1389: Reserved for future codification purposes.

#### Part 9. Criminal Justice Information.

#### § 143B-1390. Definitions.

As used in this Part:

- (1) "Board" means the Criminal Justice Information Network Governing Board established by G.S. 143B-1391.
- (2) "Local government user" means a unit of local government of this State having authorized access to the Network.
- (3) "Network" means the Criminal Justice Information Network established by the Board pursuant to this Part.
- (4) "Network user" or "user" means any person having authorized access to the Network.
- (5) "State agency" means any State department, agency, institution, board, commission, or other unit of State government. (1996, 2nd Ex. Sess., c. 18, s. 23.3(a); 2015-241, s. 7A.3(1).)

#### § 143B-1391. Criminal Justice Information Network Governing Board – creation; purpose; membership; conflicts of interest.

(a) The Criminal Justice Information Network Governing Board is established within the Department of Information Technology, as a Type II transfer, to operate the State's Criminal Justice Information Network, the purpose of which shall be to provide the governmental and technical information systems infrastructure necessary for accomplishing State and local governmental public safety and justice functions in the most effective manner by appropriately and efficiently sharing criminal justice and juvenile justice information among law enforcement, judicial, and corrections agencies. The Board is established within the Office of the State Chief Information Officer, for organizational and budgetary purposes only and the Board shall exercise all of its statutory powers in this Part independent of control by the Office of the State Chief Information Officer.

- (b) The Board shall consist of 21 members, appointed as follows:
- (1) Five members appointed by the Governor, including one member who is a director or employee of a State correction agency for a term to begin September 1, 1996 and to expire on June 30, 1997, one member who is an employee of the North Carolina Department of Public Safety for a term beginning September 1, 1996 and to expire on June 30, 1997, one member selected from the North Carolina Association of Chiefs of Police for a term to begin September 1, 1996 and to expire on June 30, 1999, one member who is an employee of the Division of Juvenile Justice of the Department of Public Safety, and one member who represents the Division of Motor Vehicles.
  - (2) Six members appointed by the General Assembly in accordance with G.S. 120-121, as follows:
    - a. Three members recommended by the President Pro Tempore of the Senate, including two members of the general public for terms to begin on September 1, 1996 and to expire on June 30, 1997, and one member selected from the North Carolina League of Municipalities who is a member of, or an employee working directly for, the governing board of a North Carolina municipality for a term to begin on September 1, 1996 and to expire on June 30, 1999; and
    - b. Three members recommended by the Speaker of the House of Representatives, including two members of the general public for terms to begin on September 1, 1996 and to expire on June 30, 1999, and one member selected from the North Carolina Association of County Commissioners who is a member of, or an employee working directly for, the governing board of a North Carolina county for a term to begin on September 1, 1996 and to expire on June 30, 1997.
  - (3) Two members appointed by the Attorney General, including one member who is an employee of the Attorney General for a term to begin on September 1, 1996 and to expire on June 30, 1997, and one member from the North Carolina Sheriffs' Association for a term to begin on September 1, 1996 and to expire on June 30, 1999.
  - (4) Six members appointed by the Chief Justice of the North Carolina Supreme Court, as follows:
    - a. The Director of the Administrative Office of the Courts, or an employee of the Administrative Office of the Courts, for a term beginning July 1, 1997, and expiring June 30, 2001.
    - b. One member who is a district attorney or an assistant district attorney upon the recommendation of the Conference of District Attorneys of North Carolina, for a term beginning July 1, 1998, and expiring June 30, 1999.
    - c. Two members who are superior court or district court judges for terms beginning July 1, 1998, and expiring June 30, 2001.
    - d. One member who is a magistrate upon the recommendation of the North Carolina Magistrates' Association, for a term beginning July 1, 1998, and expiring June 30, 1999.

- e. One member who is a clerk of superior court upon the recommendation of the North Carolina Association of Clerks of Superior Court, for a term beginning July 1, 1998, and expiring June 30, 1999.
- (5) One member appointed by the State Chief Information Officer.
- (6) One member appointed by the President of the North Carolina Chapter of the Association of Public Communications Officials International, who is an active member of the Association, for a term to begin on September 1, 1996 and to expire on June 30, 1999.

The respective appointing authorities are encouraged to appoint persons having a background in and familiarity with criminal information systems and networks generally and with the criminal information needs and capacities of the constituency from which the member is appointed.

As the initial terms expire, subsequent members of the Board shall be appointed to serve four-year terms. At the end of a term, a member shall continue to serve on the Board until a successor is appointed. A member who is appointed after a term is begun serves only for the remainder of the term and until a successor is appointed. Any vacancy in the membership of the Board shall be filled by the same appointing authority that made the appointment, except that vacancies among members appointed by the General Assembly shall be filled in accordance with G.S. 120-122.

(c) Members of the Board shall not be employed by or serve on the board of directors or other corporate governing body of any information systems, computer hardware, computer software, or telecommunications vendor of goods and services to the State or to any unit of local government in the State. No member of the Board shall vote on an action affecting solely the member's own State agency or local governmental unit or specific judicial office. (1996, 2nd Ex. Sess., c. 18, s. 23.3(a); 1998-202, s. 9; 1998-212, s. 18.2(b); 2001-424, s. 23.6(b); 2001-487, s. 90; 2003-284, s. 17.1(a); 2004-129, s. 42; 2011-145, ss. 6A.11(b), 19.1(g), (l); 2015-241, ss. 7A.2(d), 7A.3(1).)

**§ 143B-1392. Compensation and expenses of Board members; travel reimbursements.**

Members of the Board shall serve without compensation but may receive travel and subsistence as follows:

- (1) Board members who are officials or employees of a State agency or unit of local government, in accordance with G.S. 138-6.
- (2) All other Board members, at the rate established in G.S. 138-5. (1996, 2nd Ex. Sess., c. 18, s. 23.3(a); 2015-241, s. 7A.3(1).)

**§ 143B-1393. Powers and duties.**

- (a) The Board shall have the following powers and duties:
  - (1) To establish and operate the Network as an integrated system of State and local government components for effectively and efficiently storing, communicating, and using criminal justice information at the State and local levels throughout North Carolina's law enforcement, judicial, juvenile justice, and corrections agencies, with the components of the Network to include electronic devices, programs, data, and governance and to set the Network's policies and procedures.

- (2) To develop and adopt uniform standards and cost-effective information technology, after thorough evaluation of the capacity of information technology to meet the present and future needs of the State and, in consultation with the Department of Information Technology, to develop and adopt standards for entering, storing, and transmitting information in criminal justice databases and for achieving maximum compatibility among user technologies.
- (3) To identify the funds needed to establish and maintain the Network, identify public and private sources of funding, and secure funding to:
  - a. Create the Network and facilitate the sharing of information among users of the Network; and
  - b. Make grants to local government users to enable them to acquire or improve elements of the Network that lie within the responsibility of their agencies or State agencies; provided that the elements developed with the funds must be available for use by the State or by local governments without cost and the applicable State agencies join in the request for funding.
- (4) To provide assistance to local governments for the financial and systems planning for Network-related automation and to coordinate and assist the Network users of this State in soliciting bids for information technology hardware, software, and services in order to assure compliance with the Board's technical standards, to gain the most advantageous contracts for the Network users of this State, and to assure financial accountability where State funds are used.
- (5) To provide a liaison among local government users and to advocate on behalf of the Network and its users in connection with legislation affecting the Network.
- (6) To facilitate the sharing of knowledge about information technologies among users of the Network.
- (7) To take any other appropriate actions to foster the development of the Network.

(b) All grants or other uses of funds appropriated or granted to the Board shall be conditioned on compliance with the Board's technical and other standards. (1996, 2nd Ex. Sess., c. 18, s. 23.3(a); 2003-284, s. 17.2(b); 2004-129, s. 43; 2015-241, ss. 7A.2(e), 7A.3(1), 7A.4(w).)

**§ 143B-1394. Election of officers; meetings; staff, etc.**

(a) The Governor shall call the first meeting of the Board. At the first meeting, the Board shall elect a chair and a vice-chair, each to serve a one-year term, with subsequent officers to be elected for one-year terms. The Board shall hold at least two regular meetings each year, as provided by policies and procedures adopted by the Board. The Board may hold additional meetings upon the call of the chair or any three Board members. A majority of the Board membership constitutes a quorum.

(b) The staff of the Criminal Justice Information Network shall provide the Board with professional and clerical support and any additional support the Board needs to fulfill its mandate. The Board's staff shall use space provided by the Department of Information

Technology. (1996, 2nd Ex. Sess., c. 18, s. 23.3(a); 2003-284, s. 17.1(b); 2011-145, ss. 6A.11(c), 19.1(g); 2015-241, ss. 7A.2(f), 7A.3(1).)

§ 143B-1395: Reserved for future codification purposes.

§ 143B-1396: Reserved for future codification purposes.

§ 143B-1397: Reserved for future codification purposes.

§ 143B-1398: Reserved for future codification purposes.

§ 143B-1399: Reserved for future codification purposes.

#### Part 10. Emergency Telephone Service.

##### § 143B-1400. Definitions.

The following definitions apply in this Part.

- (1) 911 Board. – The 911 Board established in G.S. 143B-1401.
- (2) 911 Fund. – The North Carolina 911 Fund established in G.S. 143B-1403.
- (3) 911 State Plan. – A document prepared, maintained, and updated by the 911 Board that provides a comprehensive plan for communicating 911 call information across networks and among PSAPs, addresses all aspects of the State's 911 system, and describes the allowable uses of revenue in the 911 Fund.
- (4) 911 system. – An emergency communications system using any available technology that does all of the following:
  - a. Enables the user of a communications service connection to reach a PSAP by dialing the digits 911.
  - b. Provides enhanced 911 service.
- (5) 911 system provider. – An entity that provides a 911 system to a PSAP.
- (6) Back-up PSAP. – The capability to operate as part of the 911 System and all other features of its associated primary PSAP. The term includes a back-up PSAP that receives 911 calls only when they are transferred from the primary PSAP or on an alternate routing basis when calls cannot be completed to the primary PSAP.
- (7) Call taking. – The act of processing a 911 call for emergency assistance by a primary PSAP, including the use of 911 system equipment, call classification, location of a caller, determination of the appropriate response level for emergency responders, and dispatching 911 call information to the appropriate responder.
- (8) Commercial Mobile Radio Service (CMRS). – Defined in 47 C.F.R. § 20.3.
- (9) Communications service. – Any of the following:
  - a. The transmission, conveyance, or routing of real-time communications to a point or between or among points by or through any electronic, radio, satellite, cable, optical, microwave, wireline, wireless, Internet protocol, or other medium or method, regardless of the protocol used.

- b. The ability to receive and terminate voice calls, messages, videos, data, or other forms of communication to, from, and between the public switched telephone network, wireless networks, IP-enabled networks, or any other communications network.
  - c. Interconnected VoIP service.
- (10) Communications service connection. – Each telephone number or trunk assigned to a residential or commercial subscriber by a communications service provider, without regard to technology deployed.
  - (11) Communications service provider. – An entity that provides communications service to a subscriber.
  - (12) CMRS connection. – Each mobile handset telephone number assigned to a CMRS subscriber with a place of primary use in North Carolina.
  - (13) CMRS provider. – An entity, whether facilities-based or nonfacilities-based, that is licensed by the Federal Communications Commission to provide CMRS or that resells CMRS within North Carolina.
  - (14) Enhanced 911 service. – Directing a 911 call to an appropriate PSAP by selective routing or other means based on the geographical location from which the call originated and providing information defining the approximate geographic location and the telephone number of a 911 caller, in accordance with the FCC Order.
  - (15) Exchange access facility. – The access from a subscriber's premises to the telephone system of a service supplier. The term includes service supplier provided access lines, private branch exchange trunks, and centrex network access registers, as defined by applicable tariffs approved by the North Carolina Utilities Commission. The term does not include service supplier owned and operated telephone pay station lines, Wide Area Telecommunications Service (WATS), Foreign Exchange (FX), or incoming only lines.
  - (16) FCC Order. – The Order of the Federal Communications Commission, FCC Docket No. 94-102, adopted on December 1, 1997, and any consent decrees, rules, and regulations adopted by the Federal Communications Commission pursuant to the Order.
  - (17) GIS mapping. – Computerized geographical information that can be used to assist in locating a person who calls emergency assistance, including street centerlines, ortho photography, and oblique imaging.
  - (18) Interconnected VoIP service. – Defined in 47 C.F.R. § 9.3.
  - (19) Local exchange carrier. – An entity that is authorized to provide telephone exchange service or exchange access in North Carolina.
  - (20) Next generation 911 system. – An IP-enabled emergency communications system using Internet Protocol, or any other available technology, to enable the user of a communications service to reach an appropriate PSAP by sending the digits 911 via dialing, text, or short message service (SMS), or any other technological means.
  - (21) Next generation 911 system provider. – An entity that provides a next generation or IP-enabled 911 system to a PSAP.

- (22) Prepaid wireless telecommunications service. – A wireless telecommunications service that allows a caller to dial 911 to access the 911 system, which service must be paid for in advance and is sold in predetermined units or dollars of which the number declines with use in a known amount.
- (23) Primary PSAP. – The first point of reception of a 911 call by a public safety answering point.
- (24) Proprietary information. – Subscriber lists, technology descriptions, technical information, or trade secrets that are developed, produced, or received internally by a communications service provider or by a communications service provider's employees, directors, officers, or agents.
- (25) Public safety answering point (PSAP). – The public safety agency that receives an incoming 911 call and dispatches appropriate public safety agencies to respond to the call.
- (26) Retail transaction. – The sale of prepaid wireless telecommunications service for any purpose other than resale.
- (27) Service supplier. – An entity that provides exchange telephone service to a telephone subscriber.
- (28) Subscriber. – A person who purchases a communications service and is able to receive it or use it periodically over time.
- (29) Voice communications service. – Any of the following:
  - a. The transmission, conveyance, or routing of real-time, two-way voice communications to a point or between or among points by or through any electronic, radio, satellite, cable, optical, microwave, wireline, wireless, or other medium or method, regardless of the protocol used.
  - b. The ability to receive and terminate voice calls to and from the public switched telephone network.
  - c. Interconnected VoIP service.
- (30), (31) Repealed by Session Laws 2015-261, s. 4(a), effective January 1, 2016.
- (32) VoIP provider. – An entity that provides interconnected VoIP service. (2007-383, s. 1(a); 2010-158, s. 1; 2011-122, s. 2; 2014-66, s. 1.1; 2015-241, s. 7A.3(2); 2015-261, ss. 1(a), 4(a).)

**§ 143B-1401. 911 Board.**

(a) Membership. – The 911 Board is established in the Department of Information Technology. Neither a local government unit that receives a distribution from the fund under G.S. 143B-1406 nor a telecommunication service provider may have more than one representative on the 911 Board. The 911 Board consists of 17 members as follows:

- (1) Four members appointed by the Governor as follows:
  - a. An individual who represents a municipality where a primary PSAP is located, appointed upon the recommendation of the North Carolina League of Municipalities.
  - b. An individual who represents a county where a primary PSAP is located, appointed upon the recommendation of the North Carolina Association of County Commissioners.
  - c. An individual who represents a VoIP provider.

- d. An individual who represents the North Carolina chapter of the National Emergency Number Association (NENA).
- (2) Six members appointed by the General Assembly upon the recommendation of the Speaker of the House of Representatives as follows:
  - a. An individual who is a sheriff, appointed upon the recommendation of the North Carolina Sheriffs' Association, Inc.
  - b. An individual who represents CMRS providers operating in North Carolina.
  - c. An individual who represents the North Carolina chapter of the Association of Public Safety Communications Officials (APCO).
  - d. Two individuals who represent local exchange carriers operating in North Carolina, one of whom represents a local exchange carrier with less than 50,000 access lines.
  - e. A fire chief with experience operating or supervising a PSAP or a director/manager of a fire-based PSAP, appointed upon the recommendation of the North Carolina State Firefighters' Association.
- (3) Six members appointed by the General Assembly upon the recommendation of the President Pro Tempore of the Senate as follows:
  - a. An individual who is a chief of police, appointed upon the recommendation of the North Carolina Association of Chiefs of Police.
  - b. Two individuals who represent CMRS providers operating in North Carolina.
  - c. A Rescue or Emergency Medical Services Chief with experience operating or supervising a PSAP, appointed upon the recommendation of the North Carolina Association of Rescue and Emergency Medical Services.
  - d. Two individuals who represent local exchange carriers operating in North Carolina, one of whom represents a local exchange carrier with less than 200,000 access lines.
- (4) The State Chief Information Officer or the State Chief Information Officer's designee, who serves as the chair.

(b) Term. – A member's term is four years. No member may serve more than two terms. Members remain in office until their successors are appointed and qualified. Vacancies are filled in the same manner as the original appointment. The Governor may remove any member for misfeasance, malfeasance, or nonfeasance in accordance with G.S. 143B-13(d).

(c) Meetings. – Members of the 911 Board serve without compensation. Members receive per diem, subsistence, and travel allowances at the rate established in G.S. 138-5. A quorum of the 911 Board is nine members. The 911 Board meets upon the call of the chair.

(d) Public Servants. – The members of the 911 Board are public servants under G.S. 138A-3 and are subject to the provisions of Chapter 138A of the General Statutes. (2007-383, s. 1(a); 2010-158, s. 2(a); 2013-286, s. 2; 2015-241, ss. 7A.3(2), 7A.4(f); 2015-264, s. 46; 2016-51, s. 6.)

**§ 143B-1402. Powers and duties of the 911 Board.**

- (a) Duties. – The 911 Board has the following powers and duties:

- (1) To develop the 911 State Plan. In developing and updating the plan, the 911 Board must monitor trends in communications service technology utilized for the 911 system and in enhanced 911 service technology, investigate and incorporate GIS mapping and other resources into the plan, ensure individual PSAP plans incorporate a back-up PSAP, and formulate strategies for the efficient and effective delivery of enhanced 911 service.
- (2) To administer the 911 Fund and the monthly 911 service charge authorized by G.S. 143B-1403.
- (3) To distribute revenue in the 911 Fund to CMRS providers and PSAPs in accordance with this Part and advise CMRS providers and PSAPs of the requirements for receiving a distribution from the 911 Fund.
- (4) To establish cooperative purchasing agreements or other contracts for the procurement of goods and services, to establish policies and procedures to fund advisory services and training for PSAPs, to set operating standards for PSAPs and back-up PSAPs, and to provide funds in accordance with these policies, procedures, and standards.
- (5) To investigate the revenues and expenditures associated with the operation of a PSAP to ensure compliance with restrictions on the use of amounts distributed from the 911 Fund.
- (6) To make and enter into contracts and agreements necessary or incidental to the performance of its powers and duties under this Part and to use revenue available to the 911 Board under G.S. 143B-1404 for administrative expenses to pay its obligations under the contracts and agreements.
- (7) To use funds available to the 911 Board under G.S. 62-47 [143B-1407] to pay its obligations incurred for statewide 911 projects.
- (8) To accept gifts, grants, or other money for the 911 Fund.
- (9) To undertake its duties in a manner that is competitively and technologically neutral as to all communications service providers.
- (10) To design, create, or acquire printed or Web-based public education materials regarding the proper use of 911.
- (11) To adopt rules to implement this Part. This authority does not include the regulation of any enhanced 911 service, such as the establishment of technical standards for telecommunications service providers to deliver 911 voice and data.
- (12) To take other necessary and proper action to implement the provisions of this Part.

(b) Prohibition. – In no event shall the 911 Board or any other State agency construct, operate, or own a communications network for the purpose of providing 911 service. The 911 Board may pay private sector vendors for provisioning a communications network for the purpose of providing citizens access to 911 services and completing call-taking processes through one or more PSAPs. (2007-383, s. 1(a); 2010-158, s. 3; 2014-66, s. 1.2; 2015-241, s. 7A.3(2); 2015-261, ss. 1(b), (c), 2, 4(b).)

**§ 143B-1403. Service charge for 911 service.**

(a) Charge Imposed. – A monthly 911 service charge is imposed on each active communications service connection that provides access to the 911 system through a voice

communications service. The service charge for service other than prepaid wireless telecommunications service is seventy cents (70¢) or a lower amount set by the 911 Board under subsection (d) of this section. The service charge is payable by the subscriber to the provider of the voice communications service. The provider may list the service charge separately from other charges on the bill. Partial payments made by a subscriber are applied first to the amount the subscriber owes the provider for the voice communications service.

(b) Prepaid Wireless. – A 911 service charge is imposed on each retail purchase of prepaid wireless telecommunications service occurring in this State of seventy cents (70¢) for each retail transaction of prepaid wireless telecommunications service or a lower amount set as provided by subsection (d) of this section. The service charge is collected and remitted as provided in G.S. 143B-1414.

(c) Remittance to 911 Board. – A communications service provider must remit the service charges collected by it under subsection (a) of this section to the 911 Board. The provider must remit the collected service charges by the end of the calendar month following the month the provider received the charges from its subscribers. A provider may deduct and retain from the service charges it receives from its subscribers and remits to the 911 Board an administrative allowance equal to the greater of one percent (1%) of the amount of service charges remitted or fifty dollars (\$50.00) a month.

(d) Adjustment of Charge. – The 911 Board must monitor the revenues generated by the service charges imposed by this section. If the 911 Board determines that the rates produce revenue that exceeds or is less than the amount needed, the 911 Board may adjust the rates. The rates must ensure full cost recovery for communications service providers and for primary PSAPs over a reasonable period of time. The 911 Board must set the service charge for prepaid wireless telecommunications service at the same rate as the monthly service charge for nonprepaid service. A change in the rate becomes effective only on July 1. The 911 Board must notify providers of a change in the rates at least 90 days before the change becomes effective. The 911 Board must notify the Department of Revenue of a change in the rate for prepaid wireless telecommunications service at least 90 days before the change becomes effective. The Department of Revenue must provide notice of a change in the rate for prepaid wireless telecommunications service at least 45 days before the change becomes effective only on the Department's Web site.

(e) Collection. – A communications service provider has no obligation to take any legal action to enforce the collection of the service charge billed to a subscriber. The 911 Board may initiate a collection action, and reasonable costs and attorneys' fees associated with that collection action may be assessed against the subscriber. At the request of the 911 Board, but no more than annually, a communications service provider must report to the 911 Board the amount of the provider's uncollected service charges. The 911 Board may request, to the extent permitted by federal privacy laws, the name, address, and telephone number of a subscriber who refuses to pay the 911 service charge.

(f) Restriction. – A local government may not impose a service charge or other fee on a subscriber to support the 911 system. (2007-383, s. 1(a); 2010-158, s. 4; 2011-122, ss. 1(a), 3; 2015-241, s. 7A.3(2); 2015-261, s. 4(c).)

#### **§ 143B-1404. 911 Fund.**

(a) Fund. – The 911 Fund is created as an interest-bearing special revenue fund within the State treasury. The 911 Board administers the Fund. The 911 Board must credit to the 911

Fund all revenues remitted to it from the service charge imposed by G.S. 143B-1403 on communications service connections in the State. Revenue in the Fund may only be used as provided in this Part.

(b) Allocation of Revenues. – The 911 Board may deduct and retain for its administrative expenses a percentage of the total service charges remitted to it under G.S. 143B-1403 for deposit in the 911 Fund. The percentage may not exceed two percent (2%). The percentage is one percent (1%) unless the 911 Board sets the percentage at a different amount. The 911 Board must monitor the amount of funds required to meet its financial commitment to provide technical assistance to primary PSAPs and set the rate at an amount that enables the 911 Board to meet this commitment. The 911 Board must allocate ten percent (10%) of the total service charges to the Next Generation 911 Reserve Fund to be administered as provided in G.S. 143B-1407. The remaining revenues remitted to the 911 Board for deposit in the 911 Fund are allocated as follows:

- (1) A percentage of the funds remitted by CMRS providers, other than the funds remitted by the Department of Revenue from prepaid wireless telecommunications service, to the 911 Fund are allocated for reimbursements to CMRS providers pursuant to G.S. 143B-1405.
- (2) A percentage of the funds remitted by CMRS providers, all funds remitted by the Department of Revenue from prepaid wireless telecommunications service, and all funds remitted by all other communications service providers are allocated for monthly distributions to primary PSAPs pursuant to G.S. 143B-1406 and grants to PSAPs pursuant to G.S. 143B-1407.
- (3) The percentage of the funds remitted by CMRS providers allocated to CMRS providers and PSAPs shall be set by the 911 Board and may be adjusted by the 911 Board as necessary to ensure full cost recovery for CMRS providers and, to the extent there are excess funds, for distributions to primary PSAPs.

(c) Report. – In February of each odd-numbered year, the 911 Board must report to the Joint Legislative Commission on Governmental Operations and the Revenue Laws Study Committee. The report must contain complete information regarding receipts and expenditures of all funds received by the 911 Board during the period covered by the report, the status of the 911 system in North Carolina at the time of the report, and the results of any investigations by the Board of PSAPs that have been completed during the period covered by the report.

(d) Nature of Revenue. – The General Assembly finds that distributions of revenue from the 911 Fund are not State expenditures for the purpose of Section 5(3) of Article III of the North Carolina Constitution. Therefore, the Governor may not reduce or withhold revenue in the 911 Fund. (2007-383, s. 1(a); 2008-134, s. 1(a); 2010-158, s. 5; 2011-122, s. 4; 2011-291, s. 2.17; 2015-241, s. 7A.3(2); 2015-261, ss. 1(d), 4(d).)

#### **§ 143B-1405. Fund distribution to CMRS providers.**

(a) Distribution. – CMRS providers are eligible for reimbursement from the 911 Fund for the actual costs incurred by the CMRS providers in complying with the requirements of enhanced 911 service. Costs of complying include costs incurred for designing, upgrading, purchasing, leasing, programming, installing, testing, or maintaining all necessary data, hardware, and software required to provide service as well as the recurring and nonrecurring costs of providing the service. To obtain reimbursement, a CMRS provider must comply with all of the following:

- (1) Invoices must be sworn.
- (2) All costs and expenses must be commercially reasonable.
- (3) All invoices for reimbursement must be related to compliance with the requirements of enhanced 911 service.
- (4) Prior approval must be obtained from the 911 Board for all invoices for payment of costs that exceed the lesser of:
  - a. One hundred percent (100%) of the eligible costs allowed under this section.
  - b. One hundred twenty-five percent (125%) of the service charges remitted to the 911 Board by the CMRS provider.

(b) **Payment Carryforward.** – If the total amount of invoices submitted to the 911 Board and approved for payment in a month exceeds the amount available from the 911 Fund for reimbursements to CMRS providers, the amount payable to each CMRS provider is reduced proportionately so that the amount paid does not exceed the amount available for payment. The balance of the payment is deferred to the following month. A deferred payment accrues interest at a rate equal to the rate earned by the 911 Fund until it is paid.

(c) **Grant Reallocation.** – If the amount of reimbursements to CMRS providers approved by the 911 Board for a fiscal year is less than the amount of funds allocated for reimbursements to CMRS providers for that fiscal year, the 911 Board may reallocate part of the excess amount to the PSAP Grant and Statewide 911 Projects Account established under G.S. 143B-1407. The 911 Board may reallocate funds under this subsection only once each calendar year and may do so only within the three-month period that follows the end of the fiscal year. If the 911 Board reallocates more than a total of three million dollars (\$3,000,000) to the PSAP Grant and Statewide 911 Projects Account in a calendar year, it must consider reducing the amount of the service charge in G.S. 143B-1404 to reflect more accurately the underlying costs of providing 911 system services.

The 911 Board must make the following findings before it reallocates funds to the PSAP Grant and Statewide 911 Projects Account:

- (1) There is a critical need for additional funding for PSAPs in rural or high-cost areas to ensure that enhanced 911 service is deployed throughout the State.
- (2) The reallocation will not impair cost recovery by CMRS providers.
- (3) The reallocation will not result in the insolvency of the 911 Fund. (2007-383, s. 1(a); 2010-158, s. 6; 2015-241, s. 7A.3(2).)

**§ 143B-1406. Fund distribution to PSAPs.**

(a) **Monthly Distribution.** – The 911 Board must make monthly distributions to primary PSAPs from the amount allocated to the 911 Fund for PSAPs. A PSAP is not eligible for a distribution under this section unless it complies with the requirements of this Part, provides enhanced 911 service, and received distributions from the 911 Board in the 2008-2009 fiscal year. The Board may reduce, suspend, or terminate distributions under this subsection if a PSAP does not comply with the requirements of this Part. The Board must comply with all of the following:

- (1) **Administration.** – The Board must notify PSAPs of the estimated distributions no later than December 31 of each year. The Board must determine actual distributions no later than June 1 of each year. The Board must determine a method for establishing distributions that is equitable and sustainable and that

ensures distributions for eligible operating costs and anticipated increases for all funded PSAPs. The Board must establish a formula to determine each PSAP's base amount. The formula must be determined and published to PSAPs in the first quarter of the fiscal year preceding the fiscal year in which the formula is used. The Board may not change the funding formula for the base amount more than once every year.

- (2) Reports. – The Board must report to the Joint Legislative Commission on Governmental Operations and the Revenue Laws Study Committee within 45 days of a change in the funding formula. The report must contain a description of the differences in the old and new formulas and the projected distributions to each PSAP from the new formula.
- (3) Formula. – The funding formula established by the Board must consider all of the following:
  - a. The population of the area served by a PSAP.
  - b. PSAP reports and budgets, disbursement histories, and historical costs.
  - c. PSAP operations, 911 technologies used by the PSAP, compliance with operating standards of the 911 Board, level of service a PSAP delivers dispatching fire, emergency medical services, law enforcement, and Emergency Medical Dispatch.
  - d. The tier designation of the county in which the PSAP is located as designated in G.S. 143B-437.08.
  - e. Any interlocal government funding agreement between a primary PSAP and a secondary PSAP, if the secondary PSAP was in existence as of June 1, 2010, receives funding under the agreement, and is within the service area of the primary PSAP.
  - e1. Any expenditure authorized by the 911 Board for statewide 911 projects or the next generation 911 system.
  - f. Any other information the Board considers relevant.
- (4) Additional distributions. – In the first quarter of the Board's fiscal year, the Board must determine whether payments to PSAPs during the preceding fiscal year exceeded or were less than the eligible costs incurred by each PSAP during the fiscal year. If a PSAP receives less than its eligible costs in any fiscal year, the Board may increase a PSAP's distribution in the following fiscal year above the base amount as determined by the formula to meet the estimated eligible costs of the PSAP as determined by the Board. The Board may not distribute less than the base amount to each PSAP except as provided in subsection (c) of this section. The Board must provide a procedure for a PSAP to request a reconsideration of its distribution or eligible expenses.

(b) Percentage Designations. – The 911 Board must determine how revenue that is allocated to the 911 Fund for distribution to primary PSAPs and is not needed to make the base amount distribution required by subdivision (a)(1) of this section is to be used. The 911 Board must designate a percentage of the remaining funds to be distributed to primary PSAPs on a per capita basis and a percentage to be allocated to the PSAP Grant Account established in G.S. 143B-1407. If the 911 Board does not designate an amount to be allocated to the PSAP Grant Account, the 911 Board must distribute all of the remaining funds on a per capita basis. The 911 Board may not change the percentage designation more than once each fiscal year.

(c) Carryforward. – A PSAP may carry forward distributions for eligible expenditures for capital outlay, capital improvements, or equipment replacement. Amounts carried forward to the next fiscal year from distributions made by the 911 Board may not be used to lower the distributions in subsection (a) of this section unless the amount is greater than twenty percent (20%) of the average yearly amount distributed to the PSAP in the prior two years. The 911 Board may allow a PSAP to carry forward a greater amount without changing the PSAP's distribution.

(d) Use of Funds. – A PSAP that receives a distribution from the 911 Fund may not use the amount received to pay for the lease or purchase of real estate, cosmetic remodeling of emergency dispatch centers, hiring or compensating telecommunicators, or the purchase of mobile communications vehicles, ambulances, fire engines, or other emergency vehicles. Distributions received by a PSAP may be used only to pay for the following:

- (1) The lease, purchase, or maintenance of:
  - a. Emergency telephone equipment, including necessary computer hardware, software, and database provisioning.
  - b. Addressing.
  - c. Telecommunicator furniture.
  - d. Dispatch equipment located exclusively within a building where a PSAP or back-up PSAP is located, excluding the costs of base station transmitters, towers, microwave links, and antennae used to dispatch emergency call information from the PSAP or back-up PSAP.
- (2) The nonrecurring costs of establishing a 911 system.
- (3) Expenditures for in-State training of 911 personnel regarding the maintenance and operation of the 911 system. Allowable training expenses include the cost of transportation, lodging, instructors, certifications, improvement programs, quality assurance training, training associated with call taking, and emergency medical, fire, or law enforcement procedures, and training specific to managing a PSAP or supervising PSAP staff. Training outside the State is not an eligible expenditure unless the training is unavailable in the State or the PSAP documents that the training costs are less if received out-of-state. Training specific to the receipt of 911 calls is allowed only for intake and related call taking quality assurance and improvement. Instructor certification costs and course required prerequisites, including physicals, psychological exams, and drug testing, are not allowable expenditures.
- (4) Charges associated with the service supplier's 911 service and other service supplier recurring charges. The PSAP providing 911 service is responsible to the communications service provider for all 911 installation, service, equipment, operation, and maintenance charges owed to the communications service provider. A PSAP may contract with a communications service provider on terms agreed to by the PSAP and the provider.

(e) Local Fund. – The fiscal officer of a PSAP to whom a distribution is made under this section must deposit the funds in a special revenue fund, as defined in G.S. 159-26(b)(2), designated as the Emergency Telephone System Fund. The fiscal officer may invest money in the Fund in the same manner that other money of the local government may be invested. Income earned from the invested money in the Emergency Telephone System Fund must be credited to the Fund. Revenue deposited into the Fund must be used only as permitted in this section.

(f) Compliance. – A PSAP, or the governing entity of a PSAP, must comply with all of the following in order to receive a distribution under this section:

- (1) A county or municipality that has one or more PSAPs must submit in writing to the 911 Board information that identifies the PSAPs in the manner required by the FCC Order.
- (2) A participating PSAP must annually submit to the 911 Board a copy of its governing agency's proposed or approved budget detailing the revenues and expenditures associated with the operation of the PSAP. The PSAP budget must identify revenues and expenditures for eligible expense reimbursements as provided in this Part and rules adopted by the 911 Board.
- (3) A PSAP must be included in its governing entity's annual audit required under the Local Government Budget and Fiscal Control Act. The Local Government Commission must provide a copy of each audit of a local government entity with a participating PSAP to the 911 Board.
- (4) A PSAP must comply with all requests by the 911 Board for financial information related to the operation of the PSAP.
- (5) By July 1, 2016, a PSAP must have a plan and means for 911 call-taking in the event 911 calls cannot be received and processed in the primary PSAP. If a PSAP has made substantial progress toward implementation of the plan and means, the 911 Board may grant the PSAP an extension until July 1, 2017, to complete implementation of the plan and means. The plan must identify the alternative capability of taking the redirected 911 calls. This subdivision does not require a PSAP to construct an alternative facility to serve as a back-up PSAP.
- (6) A primary PSAP must comply with the rules, policies, procedures, and operating standards for primary PSAPs adopted by the 911 Board.

(g) Application to Cherokees. – The Eastern Band of Cherokee Indians is an eligible PSAP. The Tribal Council of the Eastern Band is the local governing entity of the Eastern Band for purposes of this section. The Tribal Council must give the 911 Board information adequate to determine the Eastern Band's base amount. The 911 Board must use the most recent federal census estimate of the population living on the Qualla Boundary to determine the per capita distribution amount. (2007-383, s. 1(a); 2008-134, ss. 1(b), (c); 2010-158, ss. 7(a)-(d); 2011-291, s. 2.18; 2014-66, s. 1.3; 2015-219, s. 1; 2015-241, s. 7A.3(2); 2015-261, ss. 1(e), 4(e).)

#### **§ 143B-1407. PSAP Grant and Statewide 911 Projects Account; Next Generation 911 Reserve Fund.**

(a) Account and Fund Established. – A PSAP Grant and Statewide 911 Projects Account is established within the 911 Fund for the purpose of making grants to PSAPs in rural and other high-cost areas and funding projects that provide statewide benefits for 911 service. The PSAP Grant and Statewide 911 Projects Account consists of revenue allocated by the 911 Board under G.S. 143B-1405(c) and G.S. 143B-1406. The Next Generation 911 Reserve Fund is established as a special fund for the purpose of funding the implementation of the next generation 911 systems as approved by the 911 Board.

(b) PSAP Grant and Statewide 911 Projects Grant Application. – A PSAP may apply to the 911 Board for a grant from the PSAP Grant and Statewide 911 Projects Account. An

application must be submitted in the manner prescribed by the 911 Board. The 911 Board may approve a grant application and enter into a grant agreement with a PSAP if it determines all of the following:

- (1) The costs estimated in the application are reasonable and have been or will be incurred for the purpose of promoting a cost-effective and efficient 911 system.
- (2) The expenses to be incurred by the applicant are consistent with the 911 State Plan.
- (3) There are sufficient funds available in the fiscal year in which the grant funds will be distributed.
- (4) The costs for consolidating one or more PSAPs with a primary PSAP, the relocation costs of primary PSAPs, or capital expenditures that enhance the 911 system, including costs not authorized under G.S. 143B-1406(d) and construction costs.

(c) PSAP Grant and Statewide 911 Projects Grant Agreement. – A PSAP Grant and Statewide 911 Projects agreement between the 911 Board and a PSAP must include the purpose of the grant, the time frame for implementing the project or program funded by the grant, the amount of the grant, and a provision for repaying grant funds if the PSAP fails to comply with any of the terms of the grant. The amount of the grant may vary among grantees. If the grant is intended to promote the deployment of enhanced 911 service in a rural area of the State, the grant agreement must specify how the funds will assist with this goal. The 911 Board must publish one or more notices each fiscal year advertising the availability of grants from the PSAP Grant and Statewide 911 Projects Account and detailing the application process, including the deadline for submitting applications, any required documents specifying costs, either incurred or anticipated, and evidence demonstrating the need for the grant. Any grant funds awarded to PSAPs under this section are in addition to any funds reimbursed under G.S. 143B-1406.

(d) Statewide 911 Projects. – The 911 Board may use funds from the PSAP Grant and Statewide 911 Projects Account and funds from the Next Generation 911 Reserve Fund for a statewide project if the Board determines the project meets all of the following requirements:

- (1) The project is consistent with the 911 plan.
- (2) The project is cost-effective and efficient when compared to the aggregated costs incurred by primary PSAPs for implementing individual projects.
- (3) The project is an eligible expense under G.S. 143B-1406(e).
- (4) The project will have statewide benefit for 911 service.

(e) Next Generation 911 Fund. – The 911 Board may use funds from the Next Generation 911 Fund to fund the implementation of next generation 911 systems. Notwithstanding Article 8 of Chapter 143C of the General Statutes, the 911 Board may expend funds from the Next Generation 911 Fund to provide for a single data network to serve PSAPs. The 911 Board may provide funds directly to PSAPs to implement next generation 911 systems. By October 1 of each year, the 911 Board must report to the Joint Legislative Commission on Governmental Operations on the expenditures from the Next Generation 911 Fund for the prior fiscal year and on the planned expenditures from the Fund for the current fiscal year. (2007-383, s. 1(a); 2010-158, s. 8; 2015-241, s. 7A.3(2); 2015-261, s. 1(f).)

**§ 143B-1408. Recovery of unauthorized use of funds.**

The 911 Board must give written notice of violation to any communications service provider or PSAP found by the 911 Board to be using monies from the 911 Fund for purposes not authorized by this Part. Upon receipt of notice, the communications service provider or PSAP must cease making any unauthorized expenditures. The communications service provider or PSAP may petition the 911 Board for a hearing on the question of whether the expenditures were unauthorized, and the 911 Board must grant the request within a reasonable period of time. If, after the hearing, the 911 Board concludes the expenditures were in fact unauthorized, the 911 Board may require the communications service provider or PSAP to refund the monies improperly spent within 90 days. Money received under this section must be credited to the 911 Fund. If a communications service provider or PSAP does not cease making unauthorized expenditures or refuses to refund improperly spent money, the 911 Board must suspend funding to the provider or PSAP until corrective action is taken. (2007-383, s. 1(a); 2015-241, s. 7A.3(2); 2015-261, s. 4(f).)

**§ 143B-1409. Conditions for providing enhanced 911 service.**

In accordance with the FCC Order, no CMRS provider is required to provide enhanced 911 service until all of the following conditions are met:

- (1) The provider receives a request for the service from the administrator of a PSAP that is capable of receiving and utilizing the data elements associated with the service.
- (2) Funds for reimbursement of the CMRS provider's costs are available pursuant to G.S. 143B-1405.
- (3) The local exchange carrier is able to support the requirements of enhanced 911 service. (2007-383, s. 1(a); 2015-241, s. 7A.3(2).)

**§ 143B-1410. Audit.**

The State Auditor may perform audits of the 911 Board pursuant to Part 5A of Chapter 147 of the General Statutes to ensure that funds in the 911 Fund are being managed in accordance with the provisions of this Part. The State Auditor must perform an audit of the 911 Board at least every two years. The 911 Board must reimburse the State Auditor for the cost of an audit of the 911 Board. (2007-383, s. 1(a); 2015-241, s. 7A.3(2).)

**§ 143B-1411. Subscriber records.**

Each CMRS provider must provide its 10,000 number groups to a PSAP upon request. This information remains the property of the disclosing CMRS provider and must be used only in providing emergency response services to 911 calls. CMRS communications service provider connection information obtained by PSAP personnel for public safety purposes is not public information under Chapter 132 of the General Statutes. No person may disclose or use, for any purpose other than the 911 system, information contained in the database of the telephone network portion of a 911 system. (2007-383, s. 1(a); 2015-241, s. 7A.3(2); 2015-261, s. 4(g).)

**§ 143B-1412. Proprietary information.**

All proprietary information submitted to the 911 Board or the State Auditor is confidential. Proprietary information submitted pursuant to this Part is not subject to disclosure under Chapter 132 of the General Statutes, and it may not be released to any person other than to the submitting communications service provider, the 911 Board, and the State Auditor without the express

permission of the submitting communications service provider. Proprietary information is considered a trade secret under the Trade Secrets Protection Act, Article 24 of Chapter 66 of the General Statutes. General information collected by the 911 Board or the State Auditor may be released or published only in aggregate amounts that do not identify or allow identification of numbers of subscribers or revenues attributable to an individual communications service provider. (2007-383, s. 1(a); 2015-241, s. 7A.3(2); 2015-261, s. 4(h).)

**§ 143B-1413. Limitation of liability.**

(a) Except in cases of wanton or willful misconduct, a communications service provider, and a 911 system provider or next generation 911 system provider, and their employees, directors, officers, vendors, and agents are not liable for any damages in a civil action resulting from death or injury to any person or from damage to property incurred by any person in connection with developing, adopting, implementing, maintaining, or operating the 911 system or in complying with emergency-related information requests from State or local government officials. This section does not apply to actions arising out of the operation or ownership of a motor vehicle. The acts and omissions described in this section include, but are not limited to, the following:

- (1) The release of subscriber information related to emergency calls or emergency services.
- (2) The use or provision of 911 service, E911 service, or next generation 911 service.
- (3) Other matters related to 911 service, E911 service, or next generation 911 service.

(b) In any civil action by a user of 911 services or next generation 911 services arising from an act or an omission by a PSAP, and the officers, directors, employees, vendors, agents, and authorizing government entity of the PSAP, in the performance of any lawful and prescribed actions pertaining to their assigned job duties as a 911 or public safety telecommunicator or dispatcher at a PSAP or at any public safety agency to which 911 calls are transferred from a primary PSAP for dispatch of appropriate public safety agencies, the plaintiff's burden of proof shall be by clear and convincing evidence. (2007-383, s. 1(a); 2015-241, s. 7A.3(2); 2015-261, s. 3.)

**§ 143B-1414. Service charge for prepaid wireless telecommunications service; seller collects 911 service charge on each retail transaction occurring in this State; remittances to Department of Revenue and transfer to 911 Fund.**

(a) Retail Collection. – A seller of prepaid wireless telecommunications service shall collect the 911 service charge for prepaid wireless telecommunications service from the consumer on each retail transaction occurring in this State. The 911 service charge for prepaid wireless telecommunications service is in addition to the sales tax imposed on the sale or recharge of prepaid telephone calling service under G.S. 105-164.4(a)(4d). The amount of the 911 service charge for prepaid wireless telecommunications service must be separately stated on an invoice, receipt, or other reasonable notification provided to the consumer by the seller at the time of the retail transaction. For purposes of this Part, a retail transaction is occurring in this State if the sale is sourced to this State under G.S. 105-164.4B(a).

(b) Administrative Allowance; Remittance to Department of Revenue. – A seller may deduct and retain from the 911 service charges it collects from consumers and remits to the

Department of Revenue an administrative allowance of five percent (5%). A seller shall remit the 911 service charge for prepaid wireless telecommunications service collected by it under subsection (a) of this section in either of the following ways:

- (1) Monthly to the Department of Revenue. The service charges collected in a month are due by the 20th day of the month following the calendar month covered by the return.
- (2) Semiannually to the Department of Revenue. The service charges collected in the first six months of the calendar year are due by July 20. The service charges collected in the second six months of the calendar year are due by January 20.

(c) Administration. – Administration, auditing, requests for review, making returns, collection of tax debts, promulgation of rules and regulations by the Secretary of Revenue, additional taxes and liens, assessments, refunds, and penalty provisions of Article 9 of Chapter 105 of the General Statutes apply to the collection of the 911 service charge for prepaid wireless telecommunications service. An audit of the collection of the 911 service charge for prepaid wireless telecommunications service shall only be conducted in connection with an audit of the taxes imposed by Article 5 of Chapter 105 of the General Statutes. Underpayments shall be subject to the same interest rate as imposed for taxes under G.S. 105-241.21. Overpayments shall be subject to the same interest rate as imposed for taxes under G.S. 105-241.21(c)(2). Excessive and erroneous collections of the service charge will be subject to G.S. 105-164.11. The Department of Revenue shall establish procedures for a seller of prepaid wireless telecommunications service to document that a sale is not a retail transaction, and the procedures established shall substantially coincide with the procedures for documenting a sale for resale transaction under G.S. 105-164.28. The Secretary of Revenue may retain the costs of collection from the remittances received under subsection (b) of this section, not to exceed five hundred thousand dollars (\$500,000) a year of the total 911 service charges for prepaid wireless telecommunications service remitted to the Department. Within 45 days of the end of each month in which 911 service charges for prepaid wireless telecommunications service are remitted to the Department, the Secretary of Revenue shall transfer the total 911 service charges remitted to the Department less the costs of collection to the 911 Fund established under G.S. 143B-1404.

(d) Liability of Consumer. – The 911 service charge for prepaid wireless telecommunications service is the liability of the consumer and not of the seller or of any provider, except that the seller shall be liable for remitting to the Department of Revenue all 911 service charges for prepaid wireless telecommunications service that the seller collects from consumers as provided in subsection (b) of this section. (2011-122, s. 5; 2013-414, s. 30; 2014-66, s. 2.1; 2015-241, s. 7A.3(2); 2016-5, ss. 3.1, 5.)

#### **§ 143B-1415. Limitation of liability, prepaid wireless.**

In addition to the limitation of liability provided in subsection G.S. 143B-1413, each provider and seller of prepaid wireless telecommunications service is entitled to the following limitations of liability:

- (1) No provider or seller of prepaid wireless telecommunications service shall be liable for damages to any person resulting from or incurred in connection with the provision of or the failure to provide 911 service, or for identifying or failing to identify the telephone number, address, location, or name associated

with any person or device that is accessing or attempting to access 911 service.

- (2) No provider or seller of prepaid wireless telecommunications service shall be liable for damages to any person resulting from or incurred in connection with the provision of any lawful assistance to any investigative or law enforcement officer of the United States, this State or any other state, or any political subdivision of this State or any other state in connection with any lawful investigation or other law enforcement activity by the law enforcement officer. (2011-122, s. 5; 2015-241, s. 7A.3(2).)

**§ 143B-1416. Exclusivity of 911 service charge for prepaid wireless telecommunications service.**

The 911 service charge for prepaid wireless telecommunications service imposed by this Part is the only 911 funding obligation imposed with respect to prepaid wireless telecommunications service in this State, and no tax, fee, surcharge, or other charge shall be imposed in this State, any subdivision of this State, or any intergovernmental agency for 911 funding purposes upon any provider, seller, or consumer with respect to the sale, purchase, use, or provision of prepaid wireless telecommunications service. (2011-122, s. 5; 2015-241, s. 7A.3(2).)

**§ 143B-1417:** Reserved for future codification purposes.

**§ 143B-1418:** Reserved for future codification purposes.

**§ 143B-1419:** Reserved for future codification purposes.

Part 11. North Carolina Geographic Information Coordinating Council.

**§ 143B-1420. Council established; role of the Center for Geographic Information and Analysis.**

(a) Council Established. – The North Carolina Geographic Information Coordinating Council ("Council") is established to develop policies regarding the utilization of geographic information, GIS systems, and other related technologies. The Council shall be responsible for the following:

- (1) Strategic planning.
- (2) Resolution of policy and technology issues.
- (3) Coordination, direction, and oversight of State, local, and private GIS efforts.
- (4) Advising the Governor, the General Assembly, and the State Chief Information Officer as to needed directions, responsibilities, and funding regarding geographic information.

The purpose of this statewide geographic information coordination effort shall be to further cooperation among State, federal, and local government agencies; academic institutions; and the private sector to improve the quality, access, cost-effectiveness, and utility of North Carolina's geographic information and to promote geographic information as a strategic resource in the State. The Council shall be located in the Office of the Governor for organizational, budgetary, and administrative purposes.

(b) Role of CGIA. – The Center for Geographic Information and Analysis (CGIA) shall staff the Geographic Information and Coordinating Council and its committees. CGIA shall

manage and distribute digital geographic information about North Carolina maintained by numerous State and local government agencies. It shall operate a statewide data clearinghouse and provide Internet access to State geographic information. (2001-359, s. 1; 2004-129, s. 44; 2015-241, s. 7A.3(3).)

**§ 143B-1421. Council membership; organization.**

(a) Members. – The Council shall consist of up to 35 members, or their designees, as set forth in this section. An appointing authority may reappoint a Council member for successive terms.

(b) Governor's Appointments. – The Governor shall appoint the following members:

- (1) The head of an at-large State agency not represented in subsection (d) of this section.
- (2) An employee of a county government, nominated by the North Carolina Association of County Commissioners.
- (3) An employee of a municipal government, nominated by the North Carolina League of Municipalities.
- (4) An employee of the federal government who is stationed in North Carolina.
- (5) A representative from the Lead Regional Organizations.
- (6) A member of the general public.
- (7) Other individuals whom the Governor deems appropriate to enhance the efforts of geographic information coordination.

Members appointed by the Governor shall serve three-year terms. The Governor shall appoint an individual from the membership of the Council to serve as Chair of the Council. The member appointed shall serve as Chair for a term of one year.

(c) General Assembly Appointments. – The President Pro Tempore of the Senate and the Speaker of the House of Representatives shall each appoint three members to the Council. These members shall serve three-year terms.

(d) Other Members. – Other Council members shall include:

- (1) The Secretary of State.
- (2) The Commissioner of Agriculture.
- (3) The Superintendent of Public Instruction.
- (4) The Secretary of Environmental Quality.
- (5) The Secretary of the Department of Transportation.
- (6) The Secretary of the Department of Administration.
- (7) The Secretary of the Department of Commerce.
- (8) The Secretary of the Department of Public Safety.
- (9) The Secretary of the Department of Health and Human Services.
- (10) The Secretary of the Department of Revenue.
- (11) The President of the North Carolina Community Colleges System.
- (12) The President of The University of North Carolina System.
- (13) The Chair of the Public Utilities Commission.
- (14) The State Budget Officer.
- (15) The Executive Director of the North Carolina League of Municipalities.
- (16) The Executive Director of the North Carolina Association of County Commissioners.
- (17) One representative from the State Government GIS User Committee.

(18) One representative elected annually from the Local Government Committee established pursuant to subdivision (h)(2) of this section.

(19) The State Chief Information Officer who shall serve as a nonvoting member.

Council members serving ex officio pursuant to this subsection shall serve terms coinciding with their respective offices. Members serving by virtue of their appointment by a standing committee of the Council shall serve for the duration of their appointment by the standing committee.

(e) Meetings. – The Council shall meet at least quarterly on the call of the Chair. The Management and Operations Committee shall conduct the Council's business between quarterly meetings.

(f) Administration. – The Director of the CGIA shall be secretary of the Council and provide staff support as it requires.

(g) Reports. – The Council shall report at least annually to the Governor and to the Joint Legislative Commission on Governmental Operations.

(h) Committees. – The Council may establish work groups, as needed, and shall oversee the standing committees created in this subsection. Each standing committee shall adopt bylaws, subject to the Council's approval, to govern its proceedings. Except as otherwise provided, the Chair of the Council shall appoint the standing committee chairs from representatives listed in subsections (b), (c), or (d) of this section. The standing committees are as follows:

(1) State Government GIS User Committee. – Membership shall consist of representatives from all interested State government departments. The Chair of the Council shall appoint the committee chair from one of the State agencies represented in subsection (d) of this section.

(2) Local Government Committee. – Membership shall consist of representatives from organizations and professional associations that currently serve or represent local government GIS users, the North Carolina League of Municipalities, the North Carolina Association of County Commissioners, and Lead Regional Organizations. The committee shall elect one of its members to the Council.

(3) Federal Interagency Committee. – Membership shall consist of representatives from all interested federal agencies and Tribal governments with an office located in North Carolina. The appointed federal representative serving pursuant to subdivision (b)(4) of this section shall serve as the Chair of the Federal Interagency Committee.

(4) Statewide Mapping Advisory Committee. – This committee shall consolidate statewide mapping requirements and attempt to gain statewide support for financing cooperative programs. The committee shall also advise the Council on issues, problems, and opportunities relating to federal, State, and local government geospatial data programs.

(5) GIS Technical Advisory Committee. – This committee shall develop the statewide technical architecture for GIS and anticipate and respond to GIS technical opportunities and issues affecting State, county, and local governments in North Carolina.

(6) Management and Operations Committee. – This committee shall consider management and operational matters related to GIS and other matters that are formally requested by the Council. The committee membership shall consist

of the Chair of the Council, the State Budget Officer, the chair of each of the standing committees of the Council, and other members of the Council appointed by the Chair. (2001-359, s. 1; 2003-340, s. 1.9; 2011-145, s. 19.1(g); 2012-120, s. 3.2; 2015-241, ss. 7A.3(3), 14.30(v).)

**§ 143B-1422. Compensation and expenses of Council members; travel reimbursements.**

Members of the Council shall serve without compensation but may receive travel and subsistence as follows:

- (1) Council members who are officials or employees of a State agency or unit of local government, in accordance with G.S. 138-6.
- (2) All other Council members at the rate established in G.S. 138-5. (2001-359, s. 1; 2015-241, s. 7A.3(3).)