Senate Bill 97

By: Senators Anavitarte of the 31st, Albers of the 56th, Dugan of the 30th, Gooch of the 51st, Robertson of the 29th and others

A BILL TO BE ENTITLED

AN ACT

To amend Chapter 3 of Title 38 of the Official Code of Georgia Annotated, relating to emergency management, so as to create the Georgia Cyber Command Division under the Georgia Emergency Management and Homeland Security Agency; to provide for definitions; to provide for the transfer of the strategic planning, facilitation, and coordination of information security in this state to the Georgia Emergency Management and Homeland Security Agency; to provide that the Governor shall appoint a state-wide chief information security officer to manage the Georgia Cyber Command Division; to provide for the powers of the Georgia Cyber Command Division; to provide for conforming changes; to provide for a short title; to provide for related matters; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Chapter 3 of Title 38 of the Official Code of Georgia Annotated, relating to emergency management, is amended by adding a new article to read as follows:

″ARTICLE 13

38-3-200.

This article shall be known and may be cited as the 'Georgia Cyber Command Act.'

38-3-201.

As used in this article, the term:

(1) 'Agency' means the Georgia Emergency Management and Homeland Security Agency.

(2) 'Breach' or 'security system breach' means an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a data base of personal information regarding multiple individuals, but shall not include a good faith acquisition of personal information by a person's employee or agent for the purposes of the person if the personal information is not used for a purpose unrelated to the person and is not subject to further unauthorized disclosure.

(3) 'CISO' means the state-wide chief information security officer.

(4) 'Director' means the director of emergency management and homeland security.

(5) 'Disaster recovery' means the measures required to mitigate the loss of information technology capability.

(6) 'Division' means the Georgia Cyber Command Division.

(7) 'Encrypt' means to use a process to transform data into a form that renders the data unreadable or unusable without using a confidential process or key.

(8) 'Information security' means the protection of information and information systems from deliberate or unintentional access, disruption, modification, or destruction by external or internal actors.

(9) 'Information technology' means all computerized and auxiliary automated information processing, telecommunications, and related technology, including hardware, software, vendor support, and related services, equipment, and projects.

(10) 'Security incident' means an event that creates reasonable suspicion that a person's information systems or computerized data may have been compromised or that measures put in place to protect the person's information systems or computerized data may have failed.

(11) 'Specified data element' means:

(A) An individual's social security number;

(B) The number on an individual's driver's license issued pursuant to Code Section 40-5-28 or nonoperating identification license issued pursuant to Code Section 40-5-100;

(C) A private key that is unique to an individual and that is used to authenticate or sign an electronic record;

(D) An individual's financial account number or credit or debit card number in combination with any required security code, access code, or password that would allow access to the individual's financial account;

(E) An individual's health insurance identification number;

(F) Information about an individual's medical or mental health treatment or diagnosis by a healthcare professional;

(G) An individual's passport number;

(H) An individual's taxpayer identification number or an identity protection personal identification number issued by the United States Internal Revenue Service; and

(I) Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

(12) 'State agency' means any authority, board, department, instrumentality, institution, agency, or other unit of state government. Such term shall not include any county, municipality, or local or regional governmental authority or the Board of Regents of the University System of Georgia.

38-3-202.

(a) On and after January 1, 2024, the agency shall be the lead state entity for the strategic planning, facilitation, and coordination of information security in this state.

(b) The powers, functions, duties, and obligations of the Georgia Technology Authority as they existed on December 31, 2023, with regard to strategic planning, facilitation, and coordination of information security pursuant to Code Section 50-25-4, are transferred to the agency effective January 1, 2024.

(c) The Governor shall appoint a state-wide CISO to manage the division. If other than the director, the CISO shall report to the director pursuant to this article.

(d) State agencies shall continue to maintain operational responsibility for their information security, to be overseen by the CISO.

38-3-203.

(a) The agency shall succeed to all rules, regulations, policies, procedures, and administrative orders of the Georgia Technology Authority that are in effect on December 31, 2023, or scheduled to go into effect on or after January 1, 2024, and which relate to the functions transferred to the agency pursuant to Code Section 38-3-202. Such rules, regulations, policies, procedures, and administrative orders shall remain in effect until amended, repealed, superseded, or nullified by the agency.

(b) The rights, privileges, entitlements, and duties of parties to contracts, leases, agreements, and other transactions entered into before January 1, 2024, by the Georgia Technology Authority which relate to the functions transferred to the agency pursuant to

Code Section 38-3-202 shall continue to exist; and none of these rights, privileges, entitlements, and duties are impaired or diminished by reason of the transfer of the functions to the agency. In all such instances, the agency shall be substituted for the Georgia Technology Authority, and the agency shall succeed to the rights and duties under such contracts, leases, agreements, and other transactions.

38-3-204.

The agency shall have the following powers with respect to the division:

(1) To establish policies and standards for state agencies to submit information security plans to the division. Such policies and standards shall include, but not be limited to, content, format, and frequency of submission;

(2) To establish information security policies, standards, and services for all state agencies, including, but not limited to, the role and responsibilities of chief information security officers within such state agencies;

(3) To advise state agencies, the judicial and legislative branches of state government, and the Board of Regents of the University System of Georgia concerning information security;

(4) To develop, implement, maintain, and ensure compliance for each state agency with state-wide information security policies and a coordinated state-wide assurance plan for information security and privacy;

(5) To direct information security and privacy protection compliance reviews for each state agency to ensure compliance with policies, standards, and effectiveness of information security assurance plans as necessary;

(6) To identify information security and privacy protection risks in each state agency and direct state agencies to adopt risk mitigation strategies, methods, and procedures to minimize the risks;

(7) To monitor and report compliance of each state agency with state information security and privacy protection policies, standards, and procedures;

(8) To coordinate state-wide information security and privacy protection awareness and training programs;

(9) To establish a State Security Operations Center for central detection, reporting, and response efforts for security incidents and breaches across the state;

(10) To adopt an information security mission statement for the State of Georgia that outlines the agency's commitment to information security, including, but not limited to, the following objectives:

(A) Fostering and developing partnerships between the division and the public and private sectors that allow for information sharing;

(B) Expanding the impact of the division beyond state agencies;

(C) Emphasizing the agency's objective for the division to protect the assets of this state and its residents, and its residents' specified data elements; and

(D) Emphasizing the agency's commitment to rapid and accurate disaster recovery by the division in the event of a security incident or security system breach;

(11) To develop other strategies as necessary to protect this state's information technology infrastructure and the data that are stored on or transmitted by the infrastructure;

(12) To operate the information security aspects of the enterprise-level infrastructure managed by the Department of Administrative Services;

(13) To consult with the Department of Administrative Services to obtain a full review of the security aspects for new and existing information technology projects;

(14) To examine all books, papers, records, and documents in the office of any state agency and require any state officer of the state agency to provide the information or statements necessary to carry out this article;

(15) To make and execute contracts, lease agreements, and all other instruments necessary or convenient to exercise the powers of the agency or to further the purpose for which the division is created;

(16) To acquire by purchase, lease, or otherwise and to hold, lease, and dispose of real or personal property of every kind and character, or any interest therein, in furtherance of the purpose of the agency;

(17) To apply for and to accept any gifts or grants or loan guarantees or loans of funds or property or financial or other aid in any form from the federal government or any federal agency or instrumentality thereof, or from the state or any state agency or instrumentality thereof, or from any other source for any or all of the purposes specified in this article and to comply, subject to the provisions of this article, with the terms and conditions thereof;

(18) To contract with state agencies or any local government for the use by the agency of any property, facilities, or services of the state or any such state agency or local government or for the use by any state agency or local government of any facilities or services of the agency; and such state agencies and local governments are authorized to enter into such contracts;

(19) To fix and collect fees and charges for data, media, and incidental services; and

(20) To do all things necessary or convenient to carry out the powers conferred by this article.

38-3-205.

The CISO may temporarily suspend operation of information infrastructure that is owned, leased, outsourced, or shared to isolate the source of, or stop the spread of, a breach or other similar security incident. A state agency and the Department of Administrative Services, as applicable, shall comply with directives to temporarily discontinue or suspend operations of information infrastructure.

38-3-206.

(a) Each state agency and its contractors shall identify and report security incidents to the division immediately on discovery and deploy disaster recovery as directed.

(b) State agencies shall demonstrate expertise to carry out security assurance plans, either by employing staff or contracting for outside services.

(c) A state agency may enter into an agreement with the agency to meet the requirements of this Code section.

38-3-207.

The CISO or any employee of the agency who knowingly divulges or makes known in any manner not permitted by law any particulars of any confidential record, document, or information is guilty of a felony and, upon conviction thereof, shall be punished by imprisonment for not less than one nor more than five years."

SECTION 2.

Chapter 25 of Title 50 of the Official Code of Georgia Annotated, relating to the Georgia Technology Authority, is amended in Code Section 50-25-4, relating to general powers, by revising subsections (9) and (20) of subsection (a) as follows:

"(9) To establish technology policies and standards for all agencies, including, but not limited to, the role and responsibilities of chief information officers ~~and chief information security officers~~ within such agencies;"

"(20) Reserved ~~To establish technology security policies, standards, and services to be used by all agencies~~;"

SECTION 3.

All laws and parts of laws in conflict with this Act are repealed.