

O.C.G.A. § 38-3-22.2

Current with Chapters 354 through 374 of the 2024 Regular Session of the General Assembly. The Statutes do not reflect possible future codification directives from the Revisor of Statutes pursuant to Code Section 28-9-5. Additionally, the Statutes may be affected by prior or subsequent legislative enactment, revision, or executive action.

Official Code of Georgia Annotated > TITLE 38 Military, Emergency Management, and Veterans Affairs (Chs. 1 — 4) > CHAPTER 3 Emergency Management (Arts. 1 — 12) > Article 2 Organization and Administration (§§ 38-3-20 — 38-3-38)

38-3-22.2. Sharing and reporting of cyber attacks and data breaches; reports or records confidential; construction with other provisions.

(a) As used in this Code section, the term:

(1) “Agency” means:

(A) The executive, judicial, or legislative branch of this state and any department, agency, board, bureau, office, commission, public corporation, and authority thereof;

(B) Every county, municipal corporation, school district, or other political subdivision of this state;

(C) Every department, agency, board, bureau, office, commission, authority, or similar body of each such county, municipal corporation, or other political subdivision of this state; and

(D) Every city, county, regional, or other authority established pursuant to the laws of this state.

Such term shall not include any county, municipal corporation, or public corporation or any authority of a county, municipal corporation, or public corporation when such county, municipal corporation, public corporation, or authority is acting in the capacity of a provider of wholesale or retail electric or gas service or in the capacity of a conduit through which a municipal corporation furnishes electric or gas service.

(2) “Utility” means any publicly, privately, or cooperatively owned line, facility, or system for producing, transmitting, or distributing power, electricity, light, heat, or gas.

(b)

(1) Except as provided in paragraph (2) of this subsection, every agency shall report to the director of emergency management and homeland security, or his or her designee, any cyber attack incident, data breach, or identified use of malware on an agency or computer or network determined by the director to be the type of cyber attack, data breach, or use of malware to

create a life-safety event, substantially impact the security of data and information systems, or affect critical systems, equipment, or service delivery.

(2) The reporting requirements of paragraph (1) of this Code section shall be satisfied if:

(A) The cyber attack incident, data breach, or identified use of malware upon an agency is of a nature required to be reported to the United States government or any agency thereof or the agency elects to report such cyber attack incident, data breach, or identified use of malware to the United States government or any agency thereof; and

(B) Within two hours of making such report to the United States government or any agency thereof, the agency provides substantially the same information to the director of emergency management and homeland security or his or her designee.

(3) The director of emergency management and homeland security shall, subject to approval by the Governor, promulgate rules and regulations specifying the reporting mechanism for making a report under paragraphs (1) and (2) of this subsection and the required information and time frame for making a report under paragraph (1) of this subsection.

(c) Every utility shall report to the director of emergency management and homeland security, or his or her designee, any cyber attack incident, data breach, or identified use of malware on a utility computer or network as such information is required to be reported to the United States government or any agency thereof. Within two hours of making such report to the United States government or any agency thereof, the utility shall provide substantially the same information to the director of emergency management and homeland security or his or her designee; provided, however, if such information is prohibited under any federal law, rule, or regulation from being disseminated, the utility shall provide such information upon the expiration or lifting of such prohibition.

(d) Any reports or records produced pursuant to this Code section shall not be subject to public inspection or disclosure under Article 4 of Chapter 18 of Title 50.

(e) Nothing in this Code section shall relieve any agency or utility of any duty that may exist under law to notify any person impacted by a cyber attack incident, data breach, or identified use of malware, including, but not limited to, any notice required under Article 34 of Chapter 1 of Title 10.

History

Code 1981, § 38-3-22.2, enacted by Ga. L. 2021, p. 11, § 1/HB 156.