Bond Case Briefs

Municipal Finance Law Since 1971

Georgia's HB 156, Requiring State Notice for Utility Cybersecurity Incidents, is Now In Effect.

Georgia's governor has signed into law House Bill 156, creating specific notice requirements for state agencies and utilities that experience cybersecurity attacks, data breaches or malware and requiring notice to the state director of emergency management in Georgia within two hours of notifying the federal emergency management agencies.

In addition, the law requires the Georgia state director of emergency management and homeland security to develop additional rules and regulations related to the notice requirements.

HB 156 was signed into law on March 25, 2021 and is already in effect.

Scope of the law

The law applies to utilities and agencies in the state of Georgia. Both terms are defined broadly:

- "**Utility"** encompasses "any publicly, privately, or cooperatively owned line, facility, or system for producing, transmitting, or distributing power, electricity, light, heat, or gas."
- **"Agency"** means Georgia "executive, judicial, or legislative branches and any department, agency, board, bureau, office, commission, public corporation, and authority; every county, municipal corporation, school district, or other political subdivision; and every department, agency, board, bureau, office, commissions, or authorities thereof; and every city, county, regional, or other authority established under Georgia law.The definition of agency specifically excludes "any county, municipal corporation, or public corporation or any authority of [the same when]…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."

Key provisions: when reports are required

The law requires utilities and agencies to make reports to the Georgia director of emergency management and homeland security in two instances:

1. Any agency must report any cyberattack incident, data breach, or identified use of malware on an agency or computer or network if the nature of the attack is determined to be of the type to "create a life-safety event, substantially impact the security of data and information systems, or affect critical systems, equipment, or service delivery." The director must develop additional requirements specifying the reporting mechanism, required information and time frame for making a report.
2. When an agency or utility is required to report a cyberattack incident, data breach, or identified use of malware on a utility or agency computer or network to the United States government or federal agency, the agency or utility must provide substantially the same information to the Georgia director of emergency management and homeland security within two hours of making a report to the United States government.

Where federal laws, rules or regulations prohibit disclosure of information that would otherwise be reportable under the law, the law permits a utility to provide the information only after the prohibition is lifted or expires.

Reports and records made under the law are exempt from state public record and FOIA laws, which proponents of the law and proposed House Bill 134 – which would permit closed government meetings when discussing cybersecurity plans and procedures – support as necessary to protect security and the interests of Georgians.

Detractors are concerned that the law and the proposed bill may erode the principles of open government. It is worth noting that the law as passed provides no specific enforcement mechanism for failure to meet the stated reporting requirements.

The trend

Although the Georgia legislature did not offer much in the way of significant commentary on this particular law, it seems likely that it was driven in part by recent high-profile cyber and ransomware attacks aimed at utilities and government agencies, including local city and country government operations.

The law appears very much in line with a federal executive order being drafted by the Biden Administration which would require both federal agencies and private entities working with the United States government to meet certain cybersecurity standards and which would mandate that private entities report any cyberattacks, breaches, or hacks to their federal government customers.

DLA Piper – Lael Bellamy and Emily Maus

May 12 2021