BARNES & THORNBURG LLP

ALERTS

New Statutory Requirements In Indiana For Reporting Cybersecurity Incidents

July 20, 2021

Highlights

Under a newly enacted state law, Indiana political subdivisions are required to report cybersecurity incidents to the Indiana Office of Technology

Each political subdivision must designate a primary reporting contact prior to Sept. 1, 2021 (and each year following before Sept. 1)

Indiana political subdivisions should understand what constitutes a cybersecurity incident and be prepared to report and address such incidents

During the 2021 legislative session, the Indiana General Assembly adopted HEA 1169, the Cyber Incident Reporting Law, which empowers the Indiana Office of Technology (IOT) to coordinate warning and preparation efforts to avoid and combat cybersecurity threats.

Pursuant to the Cyber Incident Reporting Law, Indiana political subdivisions – which the law solely applies to –will now need to comply with reporting requirements in the event a cybersecurity incident occurs. Within 48 hours of occurrence, the incident must be reported to the IOT

RELATED PEOPLE

Dustin W. Meeks
Associate
Indianapolis

P 317-231-6427
F 317-231-7433
dustin.meeks@btlaw.com

Jacob A. German
Partner
Indianapolis

P 317-231-7538
F 317-231-7433
jacob.german@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy

RELATED INDUSTRIES

Government and Public Finance

so that it may warn other units, study the incident and better prepare systems against future incidents. There are permitted delays in reporting, under the law, to avoid violations of federal privacy law and disruption of an ongoing law enforcement investigation. It is important to note that this law does not change Indiana's data breach notification law for breaches of consumer personal information in the non-political context.

A cybersecurity incident occurs when an information technology system is subject to an event which has or may imperil the system's functionality, integrity, or the security of information stored, transmitted or processed by that system. Events where a violation of a unit's policies on acceptable use and security have occurred and events which cause a risk to public health and safety are also incidents that must be reported. The law provides for the use of best professional judgment in determining if an occurrence is suspicious or malicious so as to constitute a cybersecurity incident.

Subdivisions required to report include, counties, cities, towns, townships, school corporations, library districts, fire protection districts, airport and hospital authorities, special taxing and service districts, building authorities, public transportation corporations, and any other political subdivision that can sue or be sued.

If the information systems operated by an Indiana political subdivision experience cybersecurity incidents such as a ransomware attack, a distributed denial of service attack, hacking resulting in a change to a website, compromise of email service security or email scams, or exploitation of known or previously unknown vulnerabilities in the subdivision's information technology systems and software then a report should be made of such incidents to the IOT.

Additional methods of attacking IT infrastructure may be added to the reporting requirements by the state's Chief Information Officer over time according to the law. In the event of an incident involving a political subdivision's information technology systems, those potentially impacted should consider reviewing the IOT's website should be reviewed and should also consider consulting with counsel regarding their obligation to report. Reports can be made directly to the IOT.

HEA 1169 also requires that each subdivision provide the Office of Technology with the name and contact information of a person who is authorized to act as the primary reporting contact to the IOT prior to Sept. 1, 2021 and each year following before Sept. 1.

For more information please contact the Barnes & Thornburg attorney with whom you work or Dustin Meeks at 317-231-6427 or dustin.meeks@btlaw.com, or Jacob German at 317-231-7538 or jacob.german@btlaw.com.