IOT Indiana Office of Technology
Powering a State that Works

Dear colleagues,

During the recently concluded General Assembly, legislators unanimously passed HEA 1169, which requires all political subdivisions and state agencies to report cybersecurity incidents to the Indiana Office of Technology (IOT). The law allows IOT to share anonymous attack information to warn others and provides an overview of cybersecurity attacks. Learn more about the law at https://on.in.gov/1169.

Which political subdivisions are required to report cybersecurity incidents to IOT?
Within 48 hours of discovery, the following political subdivisions are required to report:

> Counties, fire protection districts, library districts, local airport authorities, local building authorities, local hospital authorities or corporations, local housing authorities, municipalities, public transportation corporations, school corporations, special service districts, special taxing districts, townships, or other separate local governmental entities that may sue and be sued.

What is a cybersecurity incident?
A malicious or suspicious occurrence that causes one or more of the following:

- Jeopardizes or may potentially jeopardize the confidentiality, integrity, or availability of an information system, an operational system, or the information that such system processes, stores, or transmits;
- Jeopardizes or may potentially jeopardize the health and safety of the public; or
- Violates security policies, security procedures, or acceptable use policies.

Which attacks must be reported?

- Ransomware - Malicious software designed to block access to a computer system until the criminals are paid a sum of money.
- Business Email Compromise - Scams targeting organizations, government, and others, who conduct wire transfers or electronic payments. The scheme leverages email accounts of executives or high-level employees involved with wire transfer payments to do fraudulent transfers.
- Vulnerability Exploitation - Vulnerabilities in a system, including the operating system, software, or application, are leveraged to force the system to enable unauthorized activities.
- Zero-day exploitation - An unknown exploit that exposes a vulnerability in software or hardware before the vulnerability can be patched or fixed by the creator of the product.
- Distributed Denial of Service - The intentional blocking of a website or application by flooding it with data.
- Website defacement - An attack on a website that changes its visual appearance or content on a website or a web page.

How do I report an incident if I am a government entity?
Report incidents by going to https://www.in.gov/cybersecurity.

Additionally, the law requires a primary contact for each governmental organization. Organizations can provide multiple contacts as long as they are authorized to report incidents and receive any information resulting from incident reporting.

Sign up to be a point of contact for your organization: https://public.govdelivery.com/accounts/INIOT/signup/26666.

Cybersecurity incidents and attacks are on the rise. While IOT is not staffed to support local government recovery efforts, we can facilitate sharing the information so that your local government neighbors have their defenses prepared.

Thank you for your work supporting and providing service for Hoosiers.

Sincerely,
Tracy Barnes
Chief Information Officer
State of Indiana