

Cybersecurity Reporting Form

Pursuant to Ohio Revised Code (ORC) § 9.64(D), this is not a public record under ORC § 149.43.

Name of Individual Submitting the Report: _____

Title/Position: _____

Email: _____ Phone: _____

Governmental Entity / Political Subdivision: _____

Date of Incident: _____

Type of Incident (Ransomware, ACH Payment Redirect, Spearphishing, etc.):

If the entity uses UAN, has UAN been notified? Yes No n/a

Has this incident been reported to other agencies? Yes No

If yes, which ones?

FBI IC3

Ohio Homeland Security — Ohio Cyber Integration Center (OCIC)*

Local Law Enforcement (specify) _____

Other (specify) _____

Was any data compromised? Yes No

Was there a loss of funds? Yes No If yes, how much was lost? _____

Describe the event. Include as many details as possible, including what data or systems were compromised (e.g., utility payments, payroll, etc.)

Does the entity have cybersecurity insurance? Yes No

Was ransom demanded? Yes No If so, was it paid? Yes No

If yes, what is the ordinance or resolution approving the payment in the public interest?

Were cybersecurity policies and procedures in place at the time of the event? Yes No

If yes, were the procedures followed? Yes No

Since the event, have any policies or procedures been adopted or modified? Yes No

If yes, describe the new or modified policies and procedures:

*Per Ohio Revised Code § 9.64, a cybersecurity or ransomware incident is to be reported as soon as possible after discovery of the incident, but not later than 7 days after, to the Ohio Department of Homeland Security — Ohio Cyber Integration Center (OCIC), and not later than 30 days after to the Auditor of State's Office.