OHIO CYBER INCIDENT **REPORTING GUIDANCE**

homelandsecurity.ohio.gov/cyber

Local government entities must notify the OCIC, as the Ohio Homeland Security designated point of contact, for each cyber incident as soon as possible, but within 7 days.

Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC.

INCIDENT

REPORT TO OCIC

Email: OCIC@dps.ohio.gov | phone: 614-387-1089

1

OCIC completes intake form with questions on incident and resources needed

2

OCIC assigns case number and notifies key response stakeholders

3

OCIC sets up initial coordination call between impacted entity and state/federal partners

4

OCIC coordinates additional calls if or as needed

5

OCIC provides key response stakeholders with relevant information

INCIDENT

Within 7 days of the incident, impacted entity contacts OCIC

1

OCIC completes intake form with questions on incident and resources needed

OCIC staff can operate under a non-disclosure agreement (NDA) with impacted entity by request

2

OCIC assigns case number and notifies key response stakeholders

OCIC utilizes a case management system that automatically assigns a case number and captures all initial intake details to support effective coordination and response

3

OCIC sets up initial coordination call between entity and state/federal partners

- **State partners** determine if state-connected portals will be disconnected for mitigation – DAS OISP, DPS IT, DPS LEADS, Secretary of State (if election related)
- **Federal** – FBI, DHS, and CISA, if needed
- **Ohio Cyber Reserve**
  - Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC
  - Verbal Orders of the Commanding Officer (VOCO) approval is required to deploy assets
  - Other state entities will leave call once Cyber Reserve engages with entity

4

OCIC coordinates additional calls if or as needed

Calls are not limited or restricted to:

- Forensics information sharing, the logs and Tactics Techniques and Procedures (TTPs) and Indicators of Compromise (IOCs)
- Mitigative actions
- Threat actor profile sharing
- Reconnection of state service portals

5

OCIC provides key response stakeholders with relevant information

Upon final disposition, OCIC gathers information from incident After Action Reports to develop **anonymized** strategic products for prevention and protection purposes

INCIDENT INFORMATION REQUIREMENTS

Organization Information

- Organization Name
- Address/County
- Phone
- Type of Organization

Contact Information (POC)

- Name/Title
- Phone
- Email

Incident Information

- Number of devices on network?
- Does the network hold PII (personally identifiable information)?
- Does the agency have any state connected devices or terminals? (LEADS, JFS, Tax, Medicaid, etc.)
- Have they been informed?
- Date of most recent backup and is backup available on any on-prem servers?
- Is access to a clean backup available?
- Date/time of incident (or when suspicious activity began)?
- Type of incident?
- Have the infected devices been taken off the network?
- Have the infected devices been turned off?
- Does your organization have cyber insurance and have they been contacted?
- What has been done so far to mitigate the issue?
- Who else has been contacted about this incident?