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 cybersecurity or ransomware 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 casenumber and notifies key response stakeholders

3

OCIC sets up initial coordination call between 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, affected entity contacts OCIC

1

OCIC completes intake form with questions on incident and resources needed

OCIC staff operate under a non-disclosure agreement (NDA)

2

OCIC assigns case number and notifies key response stakeholders

OCIC uses a case management system that automatically generates a case number and captures all initial intake information for tracking and coordination purposes

3

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

- **State partners** determine if state-connected portals will be disconnected during mitigation – DAS OISP, DPS IT, DPS LEADS, Secretary of State (if election related)
- **Federal** – FBI, DHS, and CISA, if needed
- **Ohio Cyber Reserve**, if requested
  - Other state entities will drop once Cyber Reserve engages with entity
  - 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

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
- After Action Report

5

OCIC provides key response stakeholders with relevant information

On the determined Course of Action, Final Disposition of the incident, and gathers information provided in After Action Reports for 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

Security Team

- Number of devices on network?
- Does the network hold PPI?
- Does the agency have a LEADS device?
- If yes, has LEADS been informed?
- Date of most recent backup?

Incident Information

- Date of incident (or when suspicious activity began)?
- 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?
- What has been done so far to mitigate the issue?
- Who else has been contacted about this incident?
- Does your organization have cyber insurance?
- If yes, has your insurance been contacted?