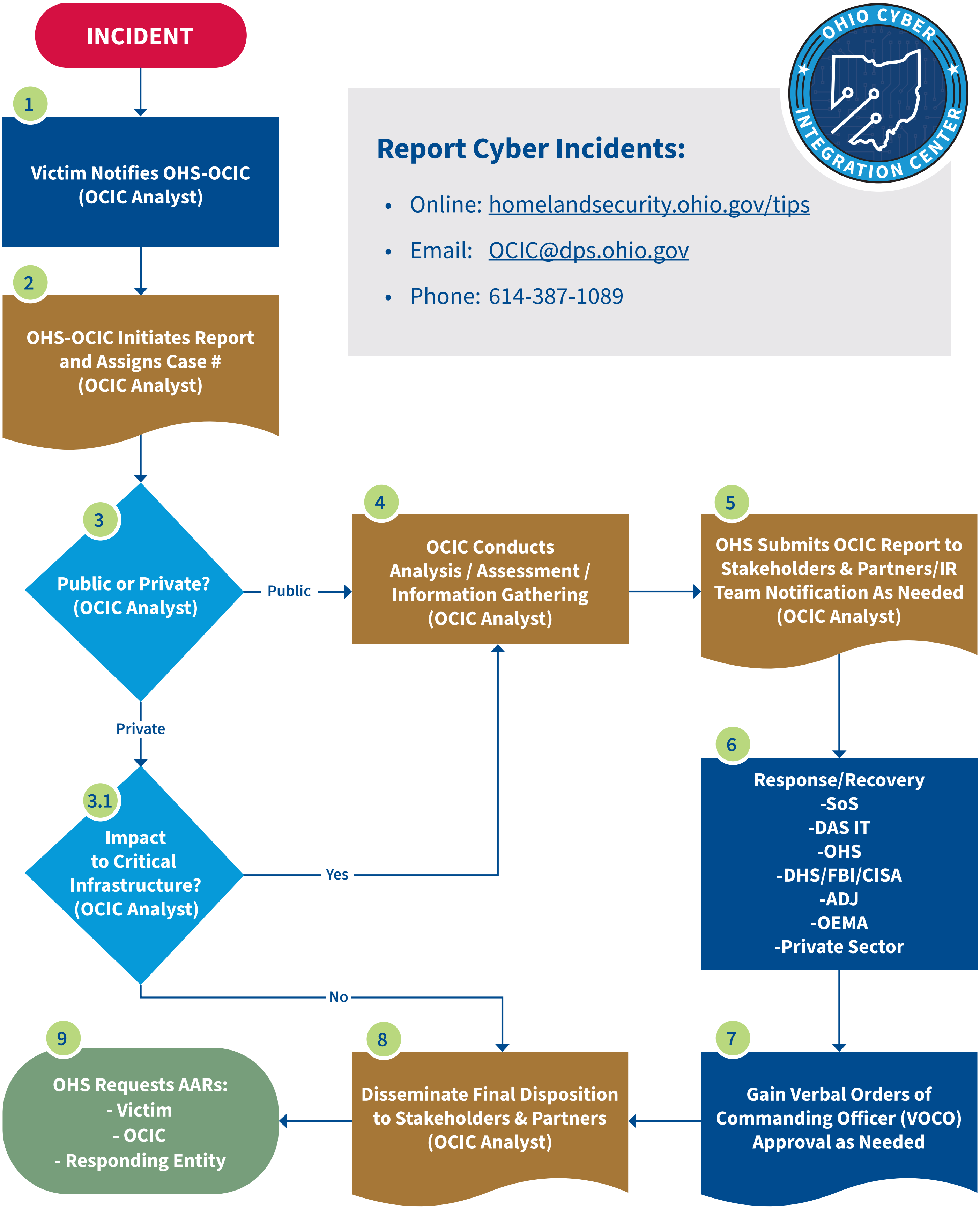
STATE CYBER INCIDENT RESPONSE

Report Cyber Incidents:

- Online: homelandsecurity.ohio.gov/tips
- Email: OCIC@dps.ohio.gov
- Phone: 614-387-1089



INCIDENT

1 Victim Notifies OHS-OCIC (OCIC Analyst)

2 OHS-OCIC Initiates Report and Assigns Case # (OCIC Analyst)

3 Public or Private? (OCIC Analyst)

3.1 Impact to Critical Infrastructure? (OCIC Analyst)

4 OCIC Conducts Analysis / Assessment / Information Gathering (OCIC Analyst)

5 OHS Submits OCIC Report to Stakeholders & Partners/IR Team Notification As Needed (OCIC Analyst)

6 Response/Recovery
-SoS
-DAS IT
-OHS
-DHS/FBI/CISA
-ADJ
-OEMA
-Private Sector

7 Gain Verbal Orders of Commanding Officer (VOCO) Approval as Needed

8 Disseminate Final Disposition to Stakeholders & Partners (OCIC Analyst)

9 OHS Requests AARs:
- Victim
- OCIC
- Responding Entity

STATE CYBER INCIDENT RESPONSE

Step 1. Victim notifies OHS-OCIC

a. OCIC Analyst gathers information from incident victim
b. If CISA/EMA makes victim first contact, they shall inform OCIC Analyst, who will contact victim for updates
c. OCIC Analyst maintains communication with victim, updates as needed

Step 2. OHS–OCIC Initiates report & assigns case#

a. OCIC Analyst assigns case#
b. OCIC Analyst sends Preliminary Email to Stakeholders
c. Incident Hour (I Hour) is time Zero (ADJ JOC starts tracking)

Step 3. Public or Private? – Decision point

Step 3.1 Impact to Critical Infrastructure – Decision point

Step 4. OCIC conducts analysis/assessment/ information gathering

a. OCIC analyst develops plan based on current information
b. IR Team notification process started as needed

Step 5. OHS Submits OCIC report to Stakeholders & Partners

a. OCIC Analyst sends final Course of Action (COA) email
b. If no message received by JOC at I+2, JOC requests updates on process from OCIC

Step 6. Response/Recovery

a. Individual agencies plan/act as required by COA Email

Step 7. Gain Verbal Orders of the Commanding Officer (VOCO) Approval as needed

a. Governor’s Office is contacted and updated
b. ADJ receives VOCO as needed & initiates action
c. All other agencies respond per protocols

Step 8. Disseminate Final Disposition to Stakeholders & Partners

a. All responding agencies report activities to OCIC Analyst
b. OCIC develops final report

Step 9. OHS requests AARs

a. All involved agencies provide AARs on all activities

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?

**Disconnected from the Internet is the best option, powering down will effect forensics of the device.*