IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

SHARING CYBER EVENT INFORMATION: OBSERVE, ACT, REPORT

April 2022

Cybersecurity information sharing is essential to collective defense and strengthening cybersecurity for the Nation. That's why, as the nation's cyber defense agency, CISA applauds the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). In accordance with CIRCIA, CISA will now undertake a rulemaking process to implement the statutory requirements. In the interim. CISA continues to encourage our stakeholders to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats to critical infrastructure. Together we can make a difference.

When cyber incidents are reported quickly, CISA can use this information to render assistance and provide a warning to prevent other organizations and entities from falling victim to a similar attack. This information is also critical to identifying trends that can help efforts to protect the homeland.

10 KEY ELEMENTS TO SHARE

* 1. Incident date and time
* 2. Incident location
* 3. Type of observed activity
* 4. Detailed narrative of the event
* 5. Number of people or systems affected
* 6. Company/Organization name
* 7. Point of Contact details
* 8. Severity of event
* 9. Critical Infrastructure Sector if known
10. Anyone else you informed

*Priority

WHAT YOU CAN DO

- **OBSERVE the activity**
- **ACT by taking local steps to mitigate the threat**
- **REPORT the event**

WHO SHOULD SHARE

- **Critical Infrastructure Owners and Operators**
- **Federal, State, Local, Territorial, and Tribal Government Partners**

WHAT TYPES OF ACTIVITY SHOULD YOU SHARE WITH CISA

- **Unauthorized access to your system**
- **Denial of Service (DOS) attacks that last more than 12 hours**
- **Malicious code on your systems, including variants if known**
- **Targeted and repeated scans against services on your systems**
- **Repeated attempts to gain unauthorized access to your system**
- **Email or mobile messages associated with phishing attempts or successes ****
- **Ransomware against Critical Infrastructure, include variant and ransom details if known**

HOW SHOULD YOU SHARE

If you are a Federal or Critical Infrastructure partner that has completed one of our Incident Reporting Forms we encourage you to continue to use this method. If you have never reported to CISA, or don't have the time or capability, we encourage you to send an email to Report@cisa.gov and be as detailed as possible using the guidelines identified above. Please include full contact information or we may not be able to take the appropriate action.

**CISA partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages, mobile messages and website locations to help people avoid becoming victims of phishing scams. You can share phishing info with CISA by sending the phishing email to phishing-report@us-cert.gov.

WHAT TO EXPECT

CISA will triage and analyze your report. If appropriate, we will share anonymized information about this activity with others to help them manage their risk. If CISA needs additional information, we will contact you for additional details from one of our official accounts.

If you have questions, contact us at (888) 282-0870 or Central@cisa.dhs.gov.