Cyber Security Services (CSS) - Security Operations Center

The CSS Security Operations Center (SOC) responds to information security incidents that potentially impact multiple agencies, or which pose a significant threat to the State of Oregon. The SOC is responsible for coordinating interagency security incident response resources and communications during or about an information security incident that impacts multiple agencies. The SOC collects, classifies, and catalogs all reported information security incidents. When an information security incident occurs that does not require SOC involvement, the SOC may assist agencies in responding to an information security incident upon request. The SOC maintains confidentiality in accordance with agency policy, rules, and legal requirements on all information security incidents reported to it.

Enterprise Information Services (EIS) through Cyber Security Services, has authority and responsibility for the statewide incident response program. The program establishes enterprise procedures, standards, and guidelines for statewide and agency-level information security incident response. The SOC maintains a forensics program capable of assisting agencies.

The SOC maintains the Statewide Incident Response Plan as well as a template for agency use to help meet their statutory obligation per ORS 276A.323. To report an incident or request a copy of the Agency Incident Response Plan template, contact the SOC using the information at the bottom of this document.

Primary responsibilities

- Vulnerability Management
    - Support the enterprise vulnerability management infrastructure
    - Enterprise uses Tenable for vulnerability scanning
    - Agencies are responsible for reviewing and patching/remediating vulnerabilities in their environment
    - Agencies are responsible for configuring scans within the agency

    - Agencies are to participate with Cybersecurity Infrastructure and Security Agency (CISA) Cyber Hygiene Scanning

- Enterprise Security Information and Event Monitoring (SIEM)
    - Enterprise uses Microsoft Sentinel SIEM with Microsoft Defender for endpoint detection and response
    - CSS SOC is solely responsible for monitoring the SIEM
    - Agencies are responsible for ensuring all systems are onboarded with Microsoft Defender
- Incident Response
    - In accordance with statewide policy 107-004-120, "Each agency must report information security incidents to CSS SOC no later than 24 hours after discovery via the CSS SOC Hotline, 503-378-5930."
    - Agencies must be familiar with the Statewide Incident Response Plan
    - Ensure the agency has an incident response plan and that it has been submitted to the CSS SOC
    - The CSS SOC maintains the Statewide Incident Response Retainer and there is no need for agencies to acquire independent IR/Forensic Response
- Phishing analysis
    - Monitoring and analyzing emails sent to the report phish mailbox
- Cybersecurity Assessments
    - Assessments are conducted every 2 years, using the Center for Internet Security (CIS) Controls

Notifying EIS Cyber Security Services (CSS) of an Incident or Cyber Disruption

When to notify

If you experienced or are experiencing an incident/cyber disruption, contact CSS within 24 hours of discovery from the phone hotline or email at the bottom of this document, whether you need assistance or not. Notification can occur at various stages, even when complete information is not available.

Notification allows correlations of cyber events across the state to identify coordinated attacks or attack trends, access to mitigation measures and expertise from similar attacks, and cyber response support.

What to report

Helpful information includes:

- Who you are
- Who experienced the incident
- What sort of incident occurred
- How and when the incident was initially detected
- What response actions have already been taken
- Who has been notified

For your situational awareness

CSS will share de-identified information with Trusted Partners for situational awareness. Trusted Partners are Oregon Emergency Management, Titan Fusion Center, Multi-State Information Sharing and Analysis Center (MS-ISAC), CISA, and National Guard.

Additional Reporting Contacts

- CISA Contacts for Reporting
    - Reporting site: https://www.cisa.gov/report
        - Direct form: https://www.cisa.gov/forms/report
        - Email: report@cisa.gov
        - Phone number: (888) 282-0870
        - The site includes reporting form, different reporting types (incident, malware, ransomware, Indicators, etc.)
- FBI Contacts for Reporting
    - Reporting site: https://www.ic3.gov/
        - Direct page: https://www.ic3.gov/Home/ComplaintChoice
        - FBI local field offices: https://www.fbi.gov/contact-us/field-offices/

- MS-ISAC Contacts for Reporting (Primarily for state, local tribal and territorial, but can contact regardless)
    - Reporting site: https://www.cisecurity.org/isac/report-an-incident
        - ISAC SOC email: soc@cisecurity.org
        - ISAC SOC phone number: (866) 787-4722

Additional Information

- For more information, please see the Guidance for State Agencies page (https://www.oregon.gov/eis/cyber-security-services/Pages/guidance-for-state-agencies.aspx for the Incident Response Plan (also found on the EIS and CSS home page), as well as the Cyber Disruption Plan page (https://www.oregon.gov/eis/cyber-security-services/Pages/cyber-disruption-plan.aspx).

Report state agency/board/commission cybersecurity incidents* at:

State SOC hotline: 503-378-5930

State SOC email: eso.soc@oregon.gov

Within 24 hours of discovery

*This is not for NOC (Network Operations Center) and local business contact. Please only use to report incidents that may impact the state environment.