Cyber Disruption Notification

When to Notify

If you are experiencing a cyber disruption, notifying CSS is recommended, 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.

Who to Notify

Cyber Security Services Security Operations Center

Email: eso_soc@oregon.gov
Phone: 503-378-5930

What to Report

Helpful information could include 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, and who has been notified.

Situational Awareness - CSS may share de-identified information with Trusted Partners for situational awareness. Trusted Partners are OEM, Titan Fusion Center, MS-ISAC, CISA, and National Guard.

Figure 2. Preferred Cyber Notification Process
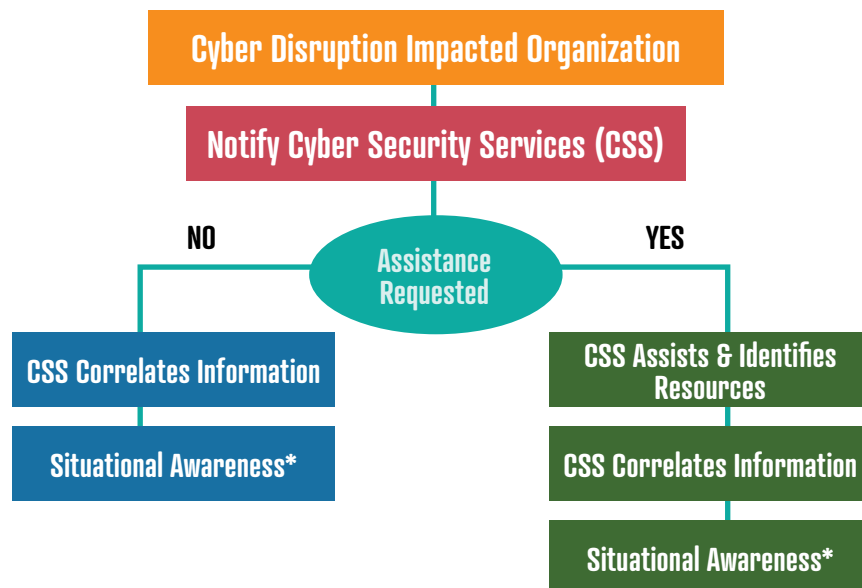
* Situational Awareness notifications may be provided to Trusted Partners (Multi-State Information Sharing and Analysis Center (MS-ISAC), Oregon Titan Fusion Center, Cybersecurity and Infrastructure Security Agency (CISA), Office of Emergency Management (OEM), Oregon National Guard (NG)) if relevant. Information in notification will be coordinated with impacted organization.