



Oregon Cyber Task Force (OCTF)

9109 NE Cascades Parkway
Portland, Oregon 97220
(503) 460-8000

Purpose

The purpose of the OCTF is to provide a statewide resource dedicated to the investigation of complex computer intrusions and digital crimes, and to enhance the cyber investigative capabilities of law enforcement agencies in Oregon through training, intelligence sharing and joint investigations.

Types of Investigations

- Theft of Personally Identifiable Information (PII) as a result of a computer intrusion;
- Destruction or loss of data from ransomware or other malicious exploits;
- Network investigations, including significant Denial of Service (DoS) attacks;
- Electronic crimes resulting from theft and sale of PII, including credit card fraud, cash-out services and retail theft;
- Complex computer intrusions conducted by state-sponsored actors or organized crime groups;
- Exploitation of vulnerabilities in critical infrastructure control systems;
- Network sabotage conducted by credentialed insiders

Support to Oregon Law Enforcement

- The OCTF can provide guidance to law enforcement agencies on response procedures for cyber crimes, to preserve evidence and enable the identification of investigative leads.
- OCTF investigators can be deployed to assist in the investigation of complex computer intrusions and significant cyber crimes.
- OCTF investigators will engage in regional training events, including table top exercises, threat intelligence briefings and cyber investigative skills.
- The OCTF will disseminate cyber criminal intelligence relating to specific threats and mitigation procedures.