APPENDIX C

State Services

CSS Services

PROACTIVE

- **Security Vendor Contracts** – Purchase agreements are made available for risk assessments, training, monitoring & detecting, response & recovery planning, and incident response. Most agreements are available to Oregon Cooperative Procurement Program intergovernmental members.
- **Cyber Security Awareness, Training, and Education** – Awareness and educational resources are offered as well as periodic technical training at a reduced rate to government organizations.

REACTIVE

- **Incident Response** – Assist government organizations with cyber response and recovery including; but not limited to, identifying and coordinating available resources, forensic analysis, and mitigation recommendations.

CONTACT

General Information

Email: eso.info@oregon.gov

Security Operations Center

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

ADDITIONAL RESOURCES

Oregon Cooperative Procurement Program
www.oregon.gov/das/procurement/pages/orcppwhat.aspx

OCDR (under development)
security.oregon.gov/cyberdisruption

Fusion Center

Fusion Center Fusion center coordinates various levels of state government, private sector entities, and the public.

PROACTIVE

- **Host/facilitate trainings** that provide proactive instruction to cyber security professionals.
- **Distribute awareness information** for cybersecurity professionals including upcoming trainings, as well as information on new malware/ransomware, etc.
- **Facilitate cross-sector information sharing** on a regular basis between various state and federal organizations.

REACTIVE

- **Correlate reports** of cyber security vulnerabilities and/or incidents and report information to appropriate authorities (typically CISA, CSS SOC, or both).
- **Share trends** and patterns in cybersecurity bulletins for our recipients' situational awareness.

CONTACT

General Information

Website: https://justice.oregon.gov/ortitan
Email: oregonfusioncenter@doj.state.or.us
Phone 877-620-4700

Oregon Office of Emergency Management

OEM is statutorily responsible for coordination of the state's emergency management program.

REACTIVE

- Coordinates emergency declarations

CONTACT

OEM Executive Duty Officer

Website: https://www.oregon.gov/oem
OpsCenter website: https://oregonem.com
Email: edo@state.or.us
Phone: 1-800-452-031

National Guard

PROACTIVE

- **Defensive Cyber Operations Element (DCO-E)** – The Oregon National Guard has a team of trained cyber personnel called the Defensive Cyber Operations Element (DCO-E). Members of the DCO-E are trained to conduct cyber vulnerability assessments, policy and process reviews, cyber audits, Continuity of Operations (COOP) planning, disaster recovery planning, cyber awareness training, tabletop exercises, threat emulation, penetration testing, and variety of other cyber tasks.

REACTIVE

- **Incident Response –** At the direction of the Governor and the Adjutant General for Oregon, the National Guard stands ready to support the state in response to a cyber disruption. Requests for resources from the national guard should be made through OEM and the Governor. Requests may be for cyber responders and for civil support. The DCO-E from the Oregon National Guard is trained in incident response, recovery, and forensics including ICS/SCADA.

CONTACT

Joint Operations Center

Email: ng.or.orarng.list.j6-dcoe@mail.mil

Phone: 503-584-2800

Federal Services

CISA Services

All services provided at no charge

PROACTIVE

CISA HQ Cyber Services:

- **Cyber Hygiene Vulnerability Scanning –** persistent scanning service of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
- **Phishing Campaign Assessments (PCA) –** measure propensity to click on email phishing lures which increases organizational training and awareness.
- **Remote Penetration Testing (RPT) –** focuses on testing a stakeholder's internet exposure.
- Web Application Scanning (WAS) assesses the "health" of publicly accessible web applications by checking for known vulnerabilities and weak configurations
- **Risk and Vulnerability Assessments (RVA) –** combine national threat information with data collected and vulnerabilities identified through on-site assessment activities to provide tailored risk analysis reports.
- **Validated Architecture Design Reviews (VADR) –** evaluate the resiliency of a stakeholder's systems, networks and security services.

Cyber Assessments:

- **Cyber Resilience Review (CRR) self-assessment and CSA1 facilitated –** identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.
- **External Dependencies Management (MDM) CSA facilitated –** assesses the activities and practices utilized to manage risks arising from external entities with network access
- **Cyber Infrastructure Survey (CIS) CSA facilitated –** identifies controls and protective measures and provides an interactive dashboard for comparative analysis and valuation
- **Cyber Security Evaluation Tool (C-SET) self-evaluation -** detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance

Cyber Incident Response:

- **Exercise Consulting, Planning, Facilitating** and Subject Expertise Support from the CISA Regional Office
- **Exercise Consulting, Planning, Facilitating** and Subject Expertise Support from CISA HQ
- **Tabletop Exercise (TTX) in-a-box Resources –** e.g. Ransomware

1 Cyber Security Advisor, a role within CISA which brings together critical infrastructure owner/operators with federal, state, local, and other stakeholders to maximize collaboration and minimize risk on matters of homeland security or emergency management.

REACTIVE

Cyber Incident Response:

- **Contact CSA for assistance** during a cyber incident/breach

Malware Analysis:

- Email submissions to NCCIC at: submit@malware.us-cert.gov
  - Send in password-protected zip file(s). Use password "infected."
- Upload submission online: https://malware.us-cert.gov

CONTACT

Theresa A. Masse

Cyber Security Advisor, Region X (Oregon)
Cybersecurity and Infrastructure Security Agency

Website: www.cisa.gov/cybersecurity
Email: theresa.masse@cisa.dhs.gov
Mobile: 503-930-5671

ADDITIONAL RESOURCES

Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government
www.dhs.gov/sites/default/files/publications/Cyber Incident Reporting United Message.pdf

CISA Cybersecurity Training & Exercises
www.cisa.gov/cybersecurity-training-exercises

Federal Bureau of Investigation (FBI)

REACTIVE

- **Investigate** the actors behind the intrusion
- **Collect** valuable time-sensitive evidence before mitigation efforts compromise the evidentiary value.
- **Provide** valuable insight and threat intelligence during and after remediation (does not mitigate or assist in remediation)

CONTACT

SSA Gabriel Gundersen

FBI Portland
Cyber Program
9109 NE Cascades Parkway
Portland, Oregon, 97220

Incident submission website: www.ic3.gov
Phone: 503-224-4181

Multi State – Information Sharing & Analysis Center (MS-ISAC Services)

Member Services

PROACTIVE

- **Advisories** - Shares cyber threat information with members when necessary and provides members with weekly threat reports, monthly situational awareness reports, and a monthly webcast.
- **Threat Notification** - Conducts research and gather intelligence about cyber threats targeting government or government-affiliated systems. Notices are sent to impacted members based on predetermined escalation procedures.
- **Malicious Domain Blocking and Reporting (MDBR)** - MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.
- **Information Sharing, Cybersecurity Awareness, and Educatio**n - Through the Homeland Security Information Network (HSIN), MS-ISAC members can access a library of cybersecurity resources. This portal also provides contact information and allows for secure email and document sharing.
- **CIS SecureSuite Membership** - Provides access to a collection of integrated cybersecurity resources such as CIS-CAT Pro Assessor, remediation content, and CIS-CAT Pro Dashboard. CIS SecureSuite Membership is free for U.S. SLTT government organizations.
- **Network Security Monitoring (Albert)** - Albert consists of an IDS sensor that gathers network data and sends it to the MS-ISAC for analysis.
- **Consulting** - a variety of consulting services, including: Infrastructure architecture review, internal systems assessment, social engineering (phishing exercises), network penetration testing, and web application penetration testing.
- **Vulnerability Assessment** - network and web application assessments include a manual analysis and verification of vulnerabilities discovered, prioritized remediation steps, customized reporting, and remediation support.
- **Managed Security Services (MSS)** - Managed Security Services (MSS) provide 24/7 monitoring, event analysis, and notifications for multiple security devices

REACTIVE

- **Vulnerability Assessments** - For state, local, tribal, and territorial (SLTT) entities experiencing a targeted cyber threat, the MS-ISAC provides a free network and web application vulnerability assessment. These assessments include a manual analysis and verification of vulnerabilities discovered, prioritized remediation steps, customized reporting, and remediation support.
- **Incident Response** - Able to assist U.S. State, Local, Tribal, and Territorial (SLTT) entities with cybersecurity incident response. Even if your SLTT organization is not an MS-ISAC or EI-ISAC member, we encourage you to contact us.
- **Malicious Code Analysis Platform (MCAP)** - MCAP is a web-based service which allows members to submit suspicious files for analysis in a controlled and non-public fashion. MCAP also enables users to perform threat analysis based on domain, IP address, URL, HASH, and various IOCs.
- **Vulnerability Management Program (VMP)** - VMP notifies members on a monthly basis about any outdated software that could pose a threat to assets.

CONTACT

Website: www.cisecurity.org/ms-isac/
Email: services@cisecurity.org
Phone: 518-880-0699

ADDITIONAL RESOURCES

Membership
https://learn.cisecurity.org/ms-isac-registration

Best Practices
www.cisecurity.org/cybersecurity-best-practices/

Cyber Threats
www.cisecurity.org/cybersecurity-threats/