Oregon Cyber Disruption Response & Recovery

Voluntary Resource Guide for Local Government

2021

ENTERPRISE
information services

ACKNOWLEDGMENTS

The Oregon Cyber Disruption Response and Recovery (OCDR) was developed in partnership with a cross jurisdictional government working group. The working group members brought their expertise and desire to support Oregon whole-of-government when a cyber disruption occurs. The working group was compromised of representation from the following Oregon government representatives:

State

Enterprise Information Services,
Cyber Security Services
Enterprise Information Services,
Shared Services (Statewide Interoperability)
Department of Justice
Oregon Emergency Management
Oregon National Guard
Oregon Titan Fusion Center
Secretary of State

Local

City of Keizer
City of Milwaukie
City of Portland
Clackamas County
Clatsop County
Douglas County
Klamath County
Yamhill County

Federal

Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency
Federal Bureau of Investigations

TABLE OF CONTENTS

INTRODUCTION

Cyber disruptions have the potential to greatly affect Oregon citizens and businesses negatively. The Oregon Cyber Disruption Response and Recovery (OCDR) - Voluntary Resource Guide for Local Government provides a common framework for responding to cyber threats impacting Oregon government and enables all levels of Oregon government to rapidly coordinate a cyber disruption response, minimizing the impact in Oregon. There is no regulatory obligation to implement the OCDR; implementation is voluntary and intended to support Oregon whole-of-government by identifying resources, providing templates, and building community.

BACKGROUND

Cyber Event is a change in the normal behavior of a given system, process, environment or workflow. An event can be either positive or negative. An average organization experiences thousands of events every day.

Cyber incidents may interfere with government business, but scope is generally limited. Cyber incidents are more numerous and routine in nature.

Cyber disruptions are major events. A cyber disruption is not a temporary inconvenience. A cyber disruption results in the sustained impairment of a critical capability that can lead to loss of life, health or safety; disrupt local, regional or national economy; curtail basic public and private infrastructure and services; and interfere with or limit the ability of government to respond to the disruption itself.

The world is increasingly dependent on technology. Information technology (IT) systems are more complex and interconnected than ever. Likewise, malicious cyber actors are highly skilled, and the number of attacks are increasing. The attacks are sophisticated, financially rewarding, and the scope of organizations being targeted continues to broaden. Government organizations are a major target and are being targeted all day, every day.

Government needs to be prepared to respond to cyber disruptions. Given the diversity in size, scope, and resources of government organizations, being prepared can look very different from one organization to another. Government has very different roles, services to provide, and technology systems. All of this adds to the complexity of preparation.

By providing a voluntary framework, the OCDR's goal is to embrace this complexity, identify areas that can be simplified, and build community collaboration.

The OCDR should complement and enhance an organization's cyber resilience and does not negate or supersede an organization's regulatory or compliance obligations. The OCDR is community-driven and will be revised to meet community needs as necessary.

SCOPE

The intended audience for the OCDR is all levels of government within Oregon. The whole-of-government approach focuses efforts and enables partnership in response activities. Effective response is complex and calls for planning and resources to be successful. Government organizations have a shared vital interest and complementary roles and responsibilities in protecting Oregon from malicious cyber activity and managing their consequences.

The OCDR identifies resources and services available to all levels of government. Some levels of government may have addition resources and services available that are not covered. The OCDR also provides guidance to enable a coordinated Oregon whole-of-government approach to cyber response activities and coordination during a cyber incident or disruption. Determining which organizations should be involved and the roles they will play has proven challenging at all levels of government.

ROLES AND RESPONSIBILITIES

State Organizations

Oregon state government works with federal, state, and local organizations along with tribal, higher education, and private industry partners to respond to, recover, and address effects of cyber disruptions in Oregon. The state promotes collaboration between partners and their respective functions. Various government partners have responsibilities, authorities, capabilities, and resources available for cyber response. Government partners need to be prepared to unify on response activities. In some cases, regulatory or contract requirements could impose certain obligations on the affected partner, such as mandatory reporting requirements and/or security determinations. Partners should engage early and ensure actions needing approval or notification be executed in a timely manner.

Cyber Security Services (CSS), Enterprise Information Services (Oregon Chief Information Security Officer's Office)

CSS is responsible for leading the state's response to a cyber disruption at a state Executive Branch agency. State Executive Branch agencies are required to comply with rules, policies, and standards set by CSS. CSS has expertise in incident response and can help facilitate a unified response and ensure that the right combination of resources respond to a particular incident. CSS is available to advise other branches of Oregon state government as well as federal and local government organizations with cyber security.

National Guard (NG)

NG has dual state and federal roles. NG forces have expertise in critical response functions and many also have expertise and capabilities in cyber activities. At the direction of the Governor and Adjutant General, the NG may perform state missions, including supporting civil authorities in response to a cyber incident or disruption.

Oregon Office of Emergency Management (OEM)

OEM is statutorily responsible for coordination of the state's emergency management program and the state's Emergency Operations Plan (EOP). This coordinating role will be fulfilled through the state Emergency Coordination Center (ECC). The purpose of the ECC is to provide a centralized location during emergencies and disasters where state officials may coordinate activities and implement direction from the Governor to provide an integrated state response. The primary responsibility of the ECC is to provide information, policy direction, and resource coordination in response to an emergency or disaster.

Oregon Titan Fusion Center (OTFC)

OTFC sits at the intersection between federal and local law enforcement and plays a role in sharing threat-related information between federal, state, local, tribal, territorial, and/or private sector partners.

Local Organizations

In addition to local community services, many State and Federal programs are delivered at the local government level. Government interdependencies brings to the forefront the necessity to understand roles and responsibilities and collaborate.

Local governments maintain their own capabilities and resources for cyber disruption response.

Federal Organizations

The Federal Government maintains a wide range of capabilities and resources that may be needed to effectively respond to a cyber disruption.

Cybersecurity and Infrastructure Security Agency (CISA) Cyber Advisor Region X, US-DHS

CISA is the nation's risk advisor. Through CISA's efforts to understand and advise on cyber and physical risks to the nation's critical infrastructure, CISA helps partners strengthen their own capabilities. CISA connects stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn strengthening national resilience. CISA offers several cyber services, available at no charge, to help State, Local, Tribal, or Territorial Government (SLTTG) improve their cyber security posture and effectively respond to cyber incidents or disruptions.

Federal Bureau of Investigation (FBI)

Lead Federal Agency for cyber investigations whose primary role is to investigate the actors behind an intrusion. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; and facilitating information sharing and operational coordination with asset response.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Supports State, Local, Tribal and Territorial (SLTT) government security and acts as a focal point for critical information exchange and coordination between the SLTT community and the Federal Government. Every state has an MS-ISAC primary member, for Oregon, the State Chief Information Security Officer is primary.

RESOURCES AND SERVICES

When a cyber disruption happens, timely access to resources and services that can assist in the response and remediation is critical. Identifying what resources and service are available prior to the cyber disruption is optimal. Prior identification provides the organization time to proactively prioritize business needs, vet third party organizations, put in place any agreements that are required, and build trusted relationships. Trying to do all of this in a middle of a cyber disruption is difficult at best.

If an organization is in need of a cyber security service not found in the Appendix, please contact CSS SOC at eso_soc@oregon.gov or 503-378-5930 and they will help the organization in locating the needed service.

Figure 1. Service Matrix provides a high level picture of services and provider of the service available to government organizations. Appendix A provides additional details along with contact information. Oregon government organizations can utilize these resources and services and many are free of charge.

Service	State		Federal		Dual Role	
	Cyber Security Services (CSS)	Office of Emergency Management (OEM)	Cybersecurity and Infrastructure Security Agency (CISA)	Multi State-Information Sharing & Analysis Center (MSISAC)	Oregon Titan Fusion Center	Oregon National Guard
Proactive						
Advisories/Threat Notification	✓	✓	✓	✓	✓	
CIS SecureSuite Membership				✓		
Consulting				✓		
Continuity Planning						✓
Cyber Assessments			✓			✓
Cyber Exercise Planning			✓			✓
Cyber Training/Education Resources	✓		✓	✓		
Cyber Vendor Contracts						
Malicious Domain Bloacking				✓		
Managed Security Services				✓		
Network Monitoring				✓		
Penetration Testing			✓			✓
Phishing Campaign Assessments			✓			
Risk & Vulnerability Assessment			✓			
Validated Architecture Design			✓			
Vulnerability Scanning			✓	✓		
Web Application Scanning			✓			
Reactive						
Alerts	✓		✓	✓	✓	
Emergency Declaration		✓				
Incident Response Assistance	✓		✓	✓		
Malicious Code Analysis Platform				✓		
Malware Analysis			✓	✓		
Vulnerability Assessment				✓		
Vulnerability Management Program				✓		

PRINCIPLES

When assisting with a cyber disruption, care must be taken to safeguard details of the cyber disruption, as well as privacy, civil liberties, and sensitive information. Those assisting an organization should defer to the affected organization in notifying other affected entities and the public.

Response activities should be conducted in a manner to facilitate restoration and recovery of an organization that has experienced a cyber disruption, balancing investigative and security requirements, and the need to return to normal operations as quickly as possible. When multiple organizations are impacted, a collaborative and coordinated response to the cyber disruption is required.

To facilitate assistance in a timely manner, it is recommended that government organizations determine business requirements for such assistance. Potential business requirements to consider may include:

- Non-Disclosure Agreements
- Regulatory certification requirements
- Legal obligations

Appendix B contains sample templates for some of these documents. The templates are intended as sample and may be modified to meet an organization's needs.

TRAINING AND EXERCISE

Organizations are encouraged to train staff on the OCDR and their roles and responsibilities when a cyber disruption occurs. Conducting periodic OCDR exercise to test operational functionality is also encouraged. Resources for training and exercise can be found in Appendix F.

MAINTENANCE

A cross- jurisdictional, cross-functional area workgroup will be convened annually to review and update the OCDR.

APPENDIX A

Prepare for a Cyber Disruption - Steps to Take

1) **Identify your cyber response team.**

   Clarify who the key players are, outline roles and responsibilities, and clearly identify which individuals have the authority to take critical response actions. Document how to contact team members 24/7, designate an alternate for key roles, and outline a cadence for how and when the team will convene and deliver updates.

   First Response Team: Includes the Cyber Response Manager and other IT/OT security staff to investigate an incident.

   Cyber Response Steering Committee: Typically includes business executive leadership, CIO or senior IT management, information security officer, and Legal Counsel (or their designees) to confirm a cyber incident/disruption and oversee response.

   Full Cyber Response Team: A complete list of individuals and roles that can be engaged as needed to scale-up and support response such as 1) internal: Public Information Officers, Human Resources, Financial Officer, and Emergency Manager and 2) external: other government cyber response organizations, cyber insurance and law enforcement.

2) **Identify contacts and response service contracts for cybersecurity service providers and equipment vendors.**

   Keep an updated list of vendor contacts and the support they can provide if a vulnerability is identified in vendor equipment. Identify a contact person for the Internet Service Provider (ISP). If incident investigation, forensic analysis, or other forms of incident response support, is contracted out to a third party, identify the contact person, determine the process for engaging their support, and identify the person on the Cyber Response Team who is authorized to engage their services. Determine the expected response timelines for each partner.

3) **Understand systems and environment.**

   Document where system maps, logs, and inventories are kept and maintained (both online and hard copy), along with the person(s) who has the credentials to access them. Document access credentials and procedures for removing access or providing temporary access to cyber responders.

4) **Outline reporting requirements and timelines.**

   Depending on the type or severity of cyber incident/disruption, there may be requirements to report to regulatory agencies and local/state/federal officials, often within the first 24 hours, and sometimes as little as 6 hours. Determine your legal and contractual obligations to report incidents/disruptions to federal/state/local officials, insurance providers, and other third parties.

5) **Identify response procedures.**

   Document procedures for investigation and documentation, containment actions for various types of attacks, and procedures for cleaning and restoring systems. Identify and pre-position the resources needed to preserve evidence, make digital images of affected systems, and conduct a forensic analysis, either internally or with the assistance of a third-party expert.

   Identify the external response organizations—including law enforcement, information sharing organizations, and cyber mutual assistance groups—that might engage during cyber incident response, particularly for when resources and capabilities are exceeded.

   Identify key contacts within external response organizations and build personal relationships in advance. Determine how much information to share and when. Document who has the authority to engage these organizations and at what point they should be notified.

6) **Develop strategic communication procedures .**

   Identify the key internal and external communications stakeholders, what information to communicate and when, and what situations warrant internal communication with employees and public communication with citizens and the media. Develop key messages and notification templates in advance.

7) **Define legal team response.**

   Cyber response should be planned, coordinated, and executed under the guidance of the legal team. Procedures to promptly alert the legal team of a cyber incident/disruption need to be in place. To ensure compliance and preserve the legal posture, the legal team should be directly involved with the investigation, documentation, and reporting.

8) **Exercise and train staff.**

   Staff should be trained on cyber response processes and procedures regularly. Cyber response exercises or participation in industry exercises should be conducted frequently to test cyber response preparedness.

APPENDIX B

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

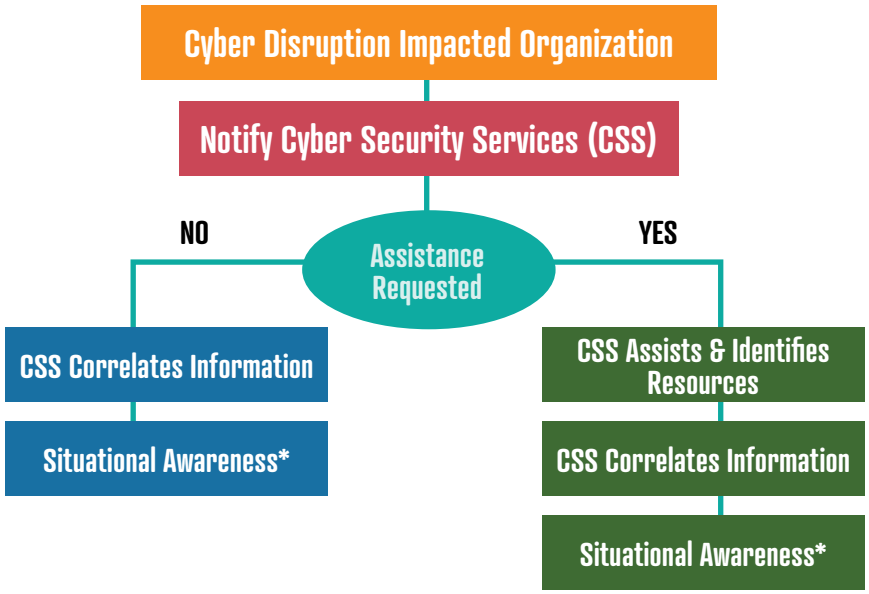
Email: eso_soc@oregon.gov
Phone: 503-378-5930

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.

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/

APPENDIX D - TEMPLATES

Templates are provided as a starting point and each organization will need to alter to fit its business need and to meet legal sufficiency.

Non-Disclosure Agreement (NDA)

Mutual Non-Disclosure and Use of Information Agreement to Support Cyber Mutual Assistance. This Non-Disclosure and Use of Information Agreement (the "Agreement'') is made and entered into as of this ___ day of ___, 20___ by and among each entity that executes and delivers the signature page to this Agreement (each, a "Participating Entity" and collectively, the "Participating Entities").

Each Participating Entity is participating in a voluntary effort to assist in developing and implementing one or more initiatives to provide cyber support assistance to participating entities.

- Each Participating Entity may voluntarily choose to request from or provide to another Participating Entity Cyber Mutual Assistance in support of cyber initiatives.
- Any request or provision of Cyber Mutual Assistance between Participating Entities may necessitate the exchange of certain confidential or proprietary information.

NOW, THEREFORE, in consideration of the mutual covenants in this Agreement, the Participating Entities agree as follows:

1) **Purpose, Scope, and Definitions.** The purpose of this Agreement is to permit each Participating Entity to exchange Confidential Information (as defined below) as needed to pursue the development and implementation of Cyber Mutual Assistance, including any request for or provision of cyber mutual assistance between Participating Entities in response to a cyber emergency or in connection with any Cyber Mutual Assistance initiative.

   "Confidential Information" under this Agreement consists of:

   A) all information disclosed by any Participating Entity, or any of its employees, directors, officers, affiliates, partners, agents, advisors or other representatives ("Representatives") pursuant to that Participating Entity's participation in or contribution to the development or implementation of Cyber Mutual Assistance, including any Participating Entity's request for or provision of cyber mutual assistance, whether disclosed prior to or following the execution of this Agreement;

   B) any information or documentation produced by a Participating Entity, or any of its Representatives, under any Cyber Mutual Assistance initiative or related to a specific request for or response to cyber mutual assistance, including any analysis of such information, and whether produced prior to or following the execution of this Agreement;

   C) any aggregation, consolidation, or listing of information or documentation disclosed by one or more Participating Entities, or any of their respective Representatives, pursuant to the development or implementation of a Cyber Mutual Assistance initiative including any Participating Entity's request for or provision of cyber mutual assistance; and

   D) all observations of equipment (including computer screens) and oral disclosures related to the development of any Cyber Mutual Assistance initiative or a specific request for or response to cyber mutual assistance, including the systems, operations, and activities of each Participating Entity, whether such observations or oral disclosures were made prior to or following the execution of this Agreement.

2) **Non-Disclosure and Use of Confidential Information.** Each Participating Entity agrees (i) to maintain the confidentiality of all Confidential Information obtained, (ii) without the express permission of the Participating Entity providing such information, not to disclose such information to third parties, and (iii) to use such information only for the express purpose of developing and implementing a Cyber Mutual Assistance initiative, including in connection with any request for or provision of cyber mutual assistance between Participating Entities. Each Participating Entity shall use the Confidential Information received hereunder only for the purposes identified in Section 1. Notwithstanding the forgoing, a Participating Entity may use and internally share Confidential Information as deemed necessary to respond to an actual or threatened cyber emergency that places, or has the potential to place, the Participating Entity's cyber systems at risk. Any other use shall be only with the prior written consent of the Participating Entity or Participating Entities that provided the Confidential Information sought to be used.

3) **Exemptions to Non-Disclosure.** Notwithstanding Sections 1 and 2, a Participating Entity shall not have breached any obligation under this Agreement if the Confidential Information is disclosed to a third party when the Confidential Information:

A) was in the public domain at the time of such disclosure or is subsequently made available to the public by the Participating Entity who provided the Confidential Information, or otherwise consistent with the terms of this Agreement; or

B) had been received or independently developed by such Participating Entity at or prior to the time of disclosure through a process other than the development or implementation of the Cyber Mutual Assistance initiative; or

C) is subsequently disclosed to the Participating Entity by a third party without restriction on use and without breach of any agreement or legal duty; or

D) subject to the provisions of Section 4, is used or disclosed pursuant to statutory duty, such as a public records act request, or an order, subpoena, discovery request, or other lawful process issued by a court or other governmental authority of competent jurisdiction or in a judicial proceeding; or

E) is disclosed by unanimous agreement of each of the Participating Entity or Participating Entities whose information is subject to such disclosure; or

F) after the time of its disclosure hereunder, becomes subsequently available to such Participating Entity on a non-confidential basis from a source not known by such Participating Entity to be bound by a confidentiality agreement or secrecy obligation in respect thereof.

4) **Notice of Pending Third-Party Disclosure or Unauthorized Disclosure**.

A) In the event that any governmental authority issues an order, subpoena, or other lawful process or a Participating Entity receives a discovery request in a civil proceeding ("Legal Process") requiring the disclosure of any Confidential Information, the Participating Entity receiving such Legal Process shall notify in writing the other Participating Entities within five (5) business days of receipt. The Participating Entity receiving such Legal Process shall not be in violation of this Agreement if it complies with the Legal Process requiring disclosure of the Confidential Information after seven (7) business days following Participating Entity notification, as set forth above.

B) A Participating Entity shall not disclose any Confidential Information in response to a request under the federal Freedom of Information Act, 5 U.S.C. § 552, as amended, or an equivalent state or local open records law, except as required by law as determined in the written opinion of such Participating Entity's legal counsel. Upon receipt of a Freedom of Information Act or public records disclosure request, such Participating Entity shall: (i) notify each Participating Entity or Participating Entities whose information is subject to such disclosure request immediately upon receipt of a request for public records that include all or part of the Confidential Information; and (ii) if, in the written opinion of the legal counsel

for the Participating Entity receiving the information request, the Confidential Information is not legally required to be disclosed, treat the requested Confidential Information as exempt from disclosure to the extent permitted by applicable law. The Participating Entity receiving the information request shall cooperate with the Participating Entity or Participating Entities whose information is subject to such disclosure requesting challenging the request or seeking another appropriate remedy, as necessary. If such challenge to the request is not successful and another remedy is not obtained, only that portion of the Confidential Information that is legally required to be disclosed, as determined in the written opinion of the Participating Entity's legal counsel, shall be disclosed.

C) Unauthorized Disclosure: If a Participating Entity becomes aware that Confidential Information has been or likely has been disclosed to a third party in violation of this Agreement, the Participating Entity will immediately notify the Participating Entity in writing that provided the disclosed Confidential Information, provide a description of the information disclosed, and provide reasonable assistance to the Participating Entity that provided the disclosed Confidential Information to recover the Confidential Information and prevent further unauthorized disclosure.

5) **Term.** This Agreement shall remain in effect as to each Participating Entity unless and until a Participating Entity seeking to withdraw from the agreement provides ten (10) days' prior written notice to the other Participating Entities, then this Agreement shall terminate with respect to such Participating Entity at the conclusion of such ten (10) day period; provided, however, that termination shall not extinguish any claim, liability, or cause of action under this Agreement existing at the time of termination. The provisions of Sections 1, 2, 3, 4, 5 and 6 shall survive the termination of this Agreement for a period of ten (10) years.

6) **Return or Destruction of Confidential Information.** Upon termination of this Agreement, all Confidential Information in the possession or control of a Participating Entity and its Representatives that received such information shall be returned to the Participating Entity that disclosed the information, including all copies of such information in any form whatsoever, unless otherwise instructed in writing by the Participating Entity that disclosed the information. Notwithstanding the foregoing, if the Confidential Information is retained in the computer backup system of a Participating

Entity, the Confidential Information will be destroyed in accordance with the regular ongoing records retention process of the Participating Entity. In lieu of return, a Participating Entity may certify to the other Participating Entities in writing that all such Confidential Information, in any form whatsoever, has been destroyed. Notwithstanding anything in this paragraph 6 to the contrary, a Participating Entity may retain a record copy of any Confidential Information if required to do so by applicable law. In such an instance, such Participating Entity shall identify in writing the specific Confidential Information retained, and shall provide the affected Participating Entity or Participating Entities with a written commitment to return or destroy the retained Confidential Information upon the expiration of the retention period required by law. The obligation under this Agreement to maintain the confidentiality of all Confidential Information shall continue to apply to such retained Confidential Information for so long as the Participating Entity possesses such Confidential Information.

7) **Notices.** All notices, requests, demands, and other communications required or permitted under this Agreement shall be in writing, unless otherwise agreed by the Participating Entities, and shall be delivered in person or sent by certified mail, postage prepaid, by overnight delivery, or by electronic mail or electronic facsimile transmission with an original sent immediately thereafter by postage prepaid mail, and properly addressed with respect to a particular Participating Entity, to such Participating Entity's representative as set forth on such Participating Entity's signature page to this Agreement. A Participating Entity may from time to time change its representative or address for the purpose of notices to that Participating Entity by a similar notice specifying a new representative or address, but no such change shall be deemed to have been given until such notice is actually received by the Participating Entity being so notified.

8) **Complete Agreement; No Other Rights.** This Agreement contains the complete and exclusive agreement of the Participating Entities with respect to the subject matter thereof. No change to this Agreement shall be effective unless agreed to in writing by all of the then existing Participating Entities. This Agreement is not intended to create any right in or obligation of any Participating Entity or third party other than those expressly stated herein.

9) **No Warranties or Representations.** Any Confidential Information disclosed under this Agreement carries no warranty or representation of any kind, either express or implied. A Participating Entity receiving such Confidential Information shall not be entitled to rely on the accuracy, completeness, or quality of the Confidential Information, even for the purpose stated in Section 1.

10) **Injunctive Relief.** Each Participating Entity agrees that, in addition to whatever other remedies may be available to the other Participating Entities under applicable law, the other Participating Entities shall be entitled to seek injunctive relief with respect to any actual or threatened violation of this Agreement by a Participating Entity or any third party receiving Confidential Information.

11) **Choice of Law and Forum**. This Agreement shall be governed by and construed in accordance with the laws of the State of Oregon without giving effect to any choice or conflicts of law provision or rule that would cause the application of laws of any other jurisdiction.

12) **Assignment.** This Agreement shall be binding upon the Participating Entities, their successors, and assigns. No Participating Entity may assign this Agreement without the prior written consent of the other Participating Entities.

13) **Construction of Agreement.** Ambiguities or uncertainties in the wording of this Agreement shall not be construed for or against any Participating Entity but shall be construed in the manner that most accurately reflects the Participating Entities' intent as of the date they executed this Agreement.

14) **Signature Authority.** Each person signing below warrants that he or she has been duly authorized by the Participating Entity for whom he or she signs to execute this Agreement on behalf of that Participating Entity.

15) **Counterparts.** This Agreement may be executed in counterparts, all of which shall be considered one and the same Agreement.

IN WITNESS WHEREOF, the Participating Entities have executed this Agreement as of the date set forth above.

Participating Entity:

By Name: _____

Title: _____

Dated: _____

By Name: _____

Title: _____

Dated: _____

Cyber Response Plan

Introduction

Note to organizations – The purpose of an cyber response program is to ensure the effective response and handling of cyber security incidents that affect the availability, integrity, or confidentiality of organization information assets. In addition, a cyber response program will ensure cyber events, incidents and vulnerabilities associated with information assets and information systems are communicated in a manner enabling timely corrective action.

This template is intended to be a guide to assist in the development of an cyber response plan, one component of an cyber response program. Organizations may have various capacities and business needs affecting the implementation of these guidelines.

<organization> has developed this Cyber Response Plan to implement its cyber response processes and procedures effectively, and to ensure that [organization] employees understand them. The intent of this document is to:

- describe the process of responding to a cyber incident,
- educate employees, and
- build awareness of security requirements.

An cyber response plan brings together and organizes the resources for dealing with any event that harms or threatens the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents, and to limit their impact while protecting information assets. The plan defines roles and responsibilities, documents the steps necessary for effectively and efficiently managing an cyber incident, and defines channels of communication. The plan also prescribes the education needed to achieve these objectives.

1) **Authority**: Provide the organizational authority such as policy, rules, or laws.
2) **Terms and Definitions**: Organizations should adjust definitions as necessary to best meet their business environment.
3) **Asset**: Anything that has value to the organization.
4) **Control**: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
5) **Cyber Response Plan**: Written document that states the approach to addressing and managing incidents.
6) **Cyber Response Procedures**: Written document(s) of the series of steps taken when responding to incidents.
7) **Cyber Security Event**: An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.
8) **Incident**: A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.
9) **Incident Response Policy**: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.
10) **Incident Response Program**: Combination of incident response policy, plan, and procedures.

11) **Information**: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication.

12) **Information Security**: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

13) **Threat**: A potential cause of an unwanted incident, which may result in harm to a system or the organization.

Roles and Responsibilities

Note to organizations – These role descriptions here are an example. Organizations should adjust these descriptions as necessary to best meet their business environment and include any additional roles that have been identified in the organization that apply such as Security Officer, Privacy Officer, etc. Organizations need to identify roles, responsibilities and identify who is responsible for incident response preparation and planning, discovery, reporting, response, investigation, recovery, follow-up and lessons learned.

Staffing will be dependent on organization's capabilities. The same person may fulfill one or more of these roles provided there is sufficient backup coverage. The following are suggested roles and responsibilities organizations should consider: incident response team members, incident commander, and point of contact to interface with external organizations.

1) **Organizations Head Executive:** Responsible for information security in the organization, for reducing risk exposure, and for ensuring the organization's activities do not introduce undue risk to the enterprise. The <Organizations Head Executive> also is responsible for ensuring compliance with security policies, standards, and security initiatives, and with local, state and federal regulations.

2) **Incident Response Point of Contact**: Responsible for communicating with external organizations and coordinating organizations actions with external organizations in response to an information security incident.

3) **Information Owner**: Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.

   User Responsible for complying with the provisions of policies, procedures and practices.

Program

Detail on organizations governance structure – identify who is responsible for managing cyber response for the organization, who is responsible for developing policy, who is responsible for developing procedures, who is responsible for awareness, identification of any governing bodies such as management committees and work groups, etc.

Include what cyber response capabilities the organization has or identify outside resource and their capabilities. Include how the organization will test plan and frequency. Include other related program areas such as business continuity planning, risk management, and privacy as they relate to incident response.

Note to organizations –Procedures may in include Incident Reporting Procedures for staff, management, information technology, and Point of Contact.

The Incident Response Program is composed of this plan in conjunction with policy and procedures. The following documents should be reviewed for a complete understanding of the program:

1) <Organization> Incident Response, Policy <XXX-XX>, located in Appendix <insert appendix number> at the end of this document.

2) <Organization> Procedure: Cyber Response, located in Appendix <insert appendix number> at the end of this document. The related flowchart for this procedure is found in Appendix <insert appendix number> at the end of this document.

Cyber incidents will be communicated in a manner allowing timely corrective action to be taken. This plan shows how the <organization> will handle response to an incident, incident communication, incident response plan testing, training for response resources and awareness training.

The Incident Response Policy, Plan, and procedures will be reviewed <insert interval here, i.e. annually> or if significant changes occur to ensure their continuing adequacy and effectiveness. Each will have an owner who has approved management responsibility for its development, review, and evaluation. Reviews will include assessing opportunities for improvement and approach to managing cyber response in regards to integrating lessons learned, to changes to <organization's> environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Identification

Identification of an incident is the process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm the <organization>. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

<Detail who is responsible for this step and the process that will be used>

The term "incident" refers to an adverse event impacting one or more <organization's> information assets or to the threat of such an event. Examples include but are not limited to the following:

- Unauthorized use
- Denial of Service
- Malicious code
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information Security Breach
- Other

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential violations of <organization's> Policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing

- Other

Incident Classification

Once an event is determined to be an incident, several methods exist for classifying incidents.

<Detail who is responsible for this step and the process that will be used>

The following factors are considered when evaluating incidents:

- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people or functions impacted
- Business considerations
- Public relations
- Enterprise impact
- Multi-agency scope

Triage

The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. It is critical to ensure when an incident is discovered and assessed the situation does not become more severe.

<Detail who is responsible for this step and the process that will be used>

- What type of incident has occurred
- Who is involved
- What is the scope
- What is the urgency
- What is the impact thus far
- What is the projected impact
- What can be done to contain the incident
- Are there other vulnerable or affected systems
- What are the effects of the incident
- What actions have been taken
- Recommendations for proceeding
- May perform analysis to identify the root cause of the incident

Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

<Detail who is responsible for this step and the process that will be used>

Forensics

Note to organizations – in cases involving potential exposure of personally identifiable information it is recommended that technical analysis be performed.

In incidents involving computers, when necessary <organization> will technically analyze computing devices to identify the cause of an incident or to analyze and preserve evidence.

<Organization> will practice the following general forensic guidelines:

- Keep good records of observations and actions taken.
- Make forensically-sound images of systems and retain them in a secure place.
- Establish chain of custody for evidence.
- Provide basic forensic training to incident response staff, especially in preservation of evidence

<Detail who is responsible for this step and the process that will be used>

Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. To do this, the vulnerability(s) needs to be clearly identified so the incident isn't repeated. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed.

<detail who is responsible for this step and the process that will be used>

Confirm that Threat/Vulnerability has been Eliminated

After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced.

<Detail who is responsible for this step and the process that will be used>

Resumption of Operations

Resuming operations is a business decision, but it is important to conduct the preceding steps to ensure it is safe to do so.

<Detail who is responsible for this step and the process that will be used>

Post-incident Activities

An after-action analysis will be performed for all incidents. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meetings should be held within one week of closing the incident.

<Detail who is responsible for this step and the process that will be used>

Education and Awareness

<Organization> shall ensure that cyber response is addressed in education and awareness programs. The programs shall address:

- <Discuss training programs, cycle/schedule, etc. Identify incident response awareness and training elements – topics to be covered, who will be trained, how much training is required.>
- <Detail training for designated response resources>

Communications

Note to organizations - Communication is vital to incident response. Therefore, it is important to control communication surrounding an incident so communications is appropriate and effective. The following aspects of incident communication should be considered:

- *Define circumstances when employees, customers and partners may or may not be informed of the issue*
- *Disclosure of incident information should be limited to a need to know basis*
- *Establish procedures for controlling communication with the media*
- *Establish procedure for communicating securely during an incident*
- *Have contact information for the external organizations and vendors contracted to help during a security emergency, as well as relevant technology providers*
- *Have contact information for customers and clients in the event they are affected by an incident*

Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must be through secure channels.

<Detail procedures for internal and external communications>

<Detail how to securely communication, what is an acceptable method>

<Detail who is responsible for communications and who is not authorized to discuss incidents>

Compliance

<Organization> is responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations.

<detail compliance objectives and initiatives>

<list policies (see authority section of plan, federal and state regulations), statutes, administrative rules that apply, etc.>

<All organization in Oregon are subject to the Oregon Consumer Information Protection Act ORS 646A.600. Breaches as defined in the Oregon Consumer Information Protection Act are only one type of an incident. If your organization is subject to the regulations list below for example, you should consider the following:

- The Payment Card Industry-Data Security Standards requires entities to develop an Incident Response Plan, require organizations to be prepared to respond immediately to a breach by following a previously developed incident response plan that addresses business recovery and continuity procedures, data backup processes, and communication and contact strategies
- HIPAA requires entities to implement policies and procedures to address security incidents, requires the creation of a security incident response team or another reasonable and appropriate response and reporting mechanism. Organizations subject to HIPAA should have both an incident response plan and an Incident response team, as well as a method to classify security incidents>

Specific to the Oregon Consumer Information Protection Act, plans should cover the following:

Consider potential communication channels for different circumstances, e.g., your plan may be different for an employee as opposed to a customer data breach.

- Your human resources office
- Public Information Officer (PIO)
- Legal Counsel
- State Of Oregon, Cyber Security Services, eso_soc@oregon.gov or 503-378-5930
- Oregon State Police – 503-378-3720 (ask for the Criminal Lieutenant)
- Other organizations that may be affected
- If security breach affects more than 1,000 consumers, contact all major consumer-reporting agencies that compile and maintain reports on consumers on a nationwide basis; inform them of the timing, distribution and content of the notification given to the consumers.
- Contact the credit monitoring bureaus in advance if directing potential victims to call them
    - Equifax – 1-800-525-6285
    - Experian – 1-888-397-3742
    - TransUnion – 1-800-680-7289

<Organization> maintains personal information of consumers and will notify customers if personal information has been subject to a security breach in accordance with the Oregon Revised Statute 646A.600 – Oregon Consumer Information Protection Act. The notification will be done as soon as possible, in one of the following manners:

- Written notification
- Electronic, if this is the customary means of communication between you and your customer, or
- Telephone notice provided that you can directly contact your customer.

Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

Substitute notice If the cost of notifying customers would exceed $250,000, that the number of those who need to be contacted is more than 350,000, or if there isn't means to sufficiently contact consumers, substitute notice will be given. Substitute notice consists of:

- Conspicuous posting of the notice or a link to the notice on your Web site if one is maintained, and
- Notification to major statewide Oregon television and newspaper media.
- *Notifying credit-reporting agencie*s If the security breach affects more than 1,000 consumers <organization> will report to all nationwide credit-reporting agencies, without reasonable delay, the timing, distribution, and the content of the notice given to the affected consumers.

<The regulations listed above are provided as examples of compliance requirements and are not intended to be a complete listing.>

Implementation

<Summary of initiatives, plans to develop tactical projects initiatives to meet plan components, including timelines, performance measures, auditing/monitoring requirements for compliance, etc.>

Approval

<Approval sign off by organizations decision makers, i.e. administrator, security officer, CIO, etc.>

By Name: _____

Title: _____

Dated: _____

By Name: _____

Title: _____

Dated: _____

APPENDIX E

Partner Organizations

Cyber Threat Intelligence Integration Center (CTIIC)

Operated by the Office of the Director of National Intelligence, the CTIIC is the primary platform for intelligence integration, analysis, and supporting activities for the Federal Government. CTIIC also provides integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests. www.dni.gov/index.php/ctiic-home

National Cybersecurity and Communications Integration Center (NCCIC)

Response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents and identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities. NCCIC assesses potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks and facilitates information sharing and operational coordination with threat response.
www.cisa.gov/national-infrastructure-coordinating-center

U.S. Cyber Command (USCYBERCOM) Joint Operations Center (JOC)

The USCYBERCOM JOC directs the U.S. military's cyberspace operations and defense of the Department of Defense Information Network (DoDIN). USCYBERCOM manages both the threat and asset responses for the DoDIN during incidents affecting the DoDIN and receives support from the other centers, as needed.
www.cybercom.mil

U.S. Secret Service

National network of Electronic Crimes Task Forces, which combine the resources of academia, the private sector, and SLTT law enforcement to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. www.secretservice.gov

United States Computer Emergency Readiness Team

United States Computer Emergency Readiness Team coordinating defense against and response to cyber attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. http://www.us-cert.gov

FirstNet

FirstNet mission is to deploy, operate, maintain, and improve the first high-speed, nationwide wireless broadband network dedicated to public safety. www.firstnet.com

APPENDIX F

References

General

OCDR website: security.oregon.gov/cyberdisruption

State of Oregon Incident Response Plan
www.oregon.gov/das/OSCIO/Documents/InformationSecurityIncidentResponsePlan.pdf

Oregon Emergency Operations Plan, Annex 10, Cyber Security
www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

Oregon cooperative procurement program
ORCPP interagency agreement template

National Cybersecurity Review (NCSR) - The Nationwide Cybersecurity Review is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of state, local, tribal and territorial governments' cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), is sponsored by the Department of Homeland Security (DHS) & the Multi-State Information Sharing and Analysis Center® (MS-ISAC®). www.cisecurity.org/ms-isac/services/ncsr/

DotGov Program, part of the General Services Administration, operates the .gov top-level domain (TLD) and makes it available to US-based government organizations, from federal agencies to local municipalities. Using a .gov domain shows you're an official government organization. https://home.dotgov.gov/

Training

Federal Emergency Management Agency (DHS/FEMA) Emergency Management Institute (EMI) offers a variety of in-residence and online courses in incident management and security and emergency management, including several on continuity and disaster recovery (www.training.DHS/FEMA.gov).

The SANS Institute provides specialized information technology training resources delivered in a variety of formats (www.sans.org).

The International Information Systems Security Certification Consortium (ISC2)offers a number of training and certification (with concentrations) options including the industry leading Certified Information Systems Security Professional (CISSP) designation (www.isc2.org)

The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans. Click here to view the FedVTE course catalog.

Exercise

The National Cybersecurity and Communications Integration Center (NCCIC) develops and supports integrated cyber incident response plans and guidance and cyber-focused exercises for governmental and critical infrastructure partners.

ENTERPRISE
information services