10

IA 10 – Cyber Security

THIS PAGE LEFT BLANK INTENTIONALLY

Table of Contents

THIS PAGE LEFT BLANK INTENTIONALLY

Primary Agencies	Department of Administrative Services (DAS)
Supporting Agencies	Oregon Office of Emergency Management (OEM)
Adjunct Agencies	

1. Introduction

A cyber-related incident may take many forms: an organized cyber-attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets. In the event of a cyber-related incident, or disaster with a cyber-component, it should be reported to Department of Administrative Services/Enterprise Security Office (DAS/ESO)

Large-scale cyber incidents may overwhelm government and private sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid threat identification, information exchange, investigation, and coordinated response and remediation are critical in cyber consequence management.

A cyber incident could seriously disrupt reliance on computers and telecommunication networks. Cyber incidents threaten the electronic infrastructure supporting the social, health, and economic well-being of Oregon's citizens. Interlinked computer networks regulate the flow of power, water, financial services, medical care, public safety, telecommunication networks and transportation systems. The consequences could cause significant disruption of operations and economic losses.

- The citizens of Oregon expect a cyber-response to effectively coordinate available assets and tools through preparation, response, mitigation and recovery from a cyber-incident.

- Cyber infrastructure: Within critical infrastructure sectors, cyber-enabled information service systems and interconnected telecommunications networks allow industrial, commercial and enterprise entities to function efficiently and expeditiously. The services are rendered through application software, proprietary access and applied security protocols including the physical layer of servers, routers, switches and transport mediums in the RF-wireless and land-based environments.
- Voice and data services are vital to Oregon's citizens to communicate with government, businesses and with each other. This critical infrastructure sector affects every resident because of the complex interdependencies

and the magnitude of telecommunications and cyber systems within Oregon.

- Disruption of critical telecommunications nodes – either physically or through cyber means – would create severe hardships until services could be restored.
- Infrastructure protection involves proactive risk management actions taken to develop ongoing preparedness initiatives that protect the specific State and sub-contracted cyber-systems from unauthorized intrusion from internal and external groups and individuals to prevent destruction of or incapacitating damage to networks and systems that serve society. Developing contingency plans to protect critical infrastructure is critical in the preparation for a cyber-incident.

2. Purpose

The purpose of this annex is to facilitate effective and coordinated State and local government response and recovery activities to cyber incidents. This Annex discusses policies, organization, actions, and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from cyber-related incidents.

These may be either statewide or national cyber-incidents impacting critical processes or economic activity.

A. Scope

This Annex provides supplemental assistance to State departments and agencies, tribal and local governments to support response activities to a cyber-incident.

- Primary cyber incident response activities for incidents limited in scope to State Executive Branch departments and agencies will be determined by the State Incident Response Team Plan in accordance with the State Information Security Incident Response Policy (107-004-120) and ORS 182.122. This annex will assist with response activities for incidents beyond the scope of those documents.
- This Annex describes the framework for Oregon State Agencies to support local units of government during a cyber-incident response.

B. Planning Assumptions

- Oregon State Agency support will coordinate response with their federal counterparts

- No single private or government agency at the local, tribal, State or Federal level possesses the authority or expertise to act unilaterally.
- A cyber incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas.
- The coordination with the Federal Government is dynamic and shaped by the nature of the event. The complexity of a cyber-annex that attempted to lay out the possible permutations and combinations of Federal/ State relations would hobble both the usefulness and maintainability of the document

This Annex is intended to develop broad concepts focused on Oregon's interface with principal Federal Agencies. Including but not limited to:

- US-DHS- Office of Cyber Security and Communications. Which includes:
  - National Communications System (NCS);
  - National Cyber Security Division;
  - Office of Emergency Communications;
  - NCS National Coordinating Center (NCC) for communications;
  - NCSD's United States Computer Emergency Readiness Team (U.S.-CERT);
  - DoD - The DoD Cyber Crime Center (DC3), U.S. Strategic Command and the subordinate U.S. Cyber Command;
  - FBI – Internet crimes

- A cyber incident will not be bounded by state or jurisdictional borders and may lack an easily identifiable signature. Cyber incidents alone, or in combination with other events, will present new and unique challenges to the State of Oregon.

- State and Local officials working with public and private partners will bring to bear critical skills required to take immediate action in identifying, responding to and recovering from a cyber-incident. These skills include:
  - Planning;
  - Risk management;
  - Threat and vulnerability identification;
  - Hazard mitigation;
  - Information security;
  - Information technology;
  - Direction, control and coordination;
  - Communications and warning;
  - Resource management;
  - Continuity of Operations (COOP)/Continuity of Government (COG);
  - Mutual Aid.

- The Oregon Cyber Annex is built on the premise that the following partners will work together to form a Unified Command utilizing the National Incident Management System (NIMS) to coordinate the actions necessary for rapid identification, information exchange, response, and remediation to mitigate the damage caused by a cyber-incident:
  - DAS
  - Oregon Military Department (OMD)/OEM
  - Other impacted State Agencies
  - Law enforcement
  - Technology resources from the private and public sectors on a case by case basis.

- This command framework may be utilized in any incident with cyber-related issues, including significant cyber threats and disruptions; crippling cyber-attacks against the Internet or critical infrastructure information systems; technologic al emergencies; or declared disasters.

- This Annex describes the specialized application of the National Response Framework (NRF) to cyber-related incidents. These cyber incidents may result in activation of the Cyber Annex and other Emergency Support Function (ESF) annexes. When processes in multiple annexes are activated, DAS continues its responsibilities under this Annex and also fulfills its responsibilities as described in other annexes to the Oregon Emergency Operations Plan.

3. Policies and Agreements

This document is not intended to establish a cyber-policy; but, rather build on fundamental policy principles and describe how organizations work collaboratively concerning cyber incidents.

- ORS 182.122 and State Information Security Incident Response Policy (107-004-120) determine responsibilities and response activities within Oregon State Executive Branch Agencies;
- Business Continuity Plan Statewide Policy ensures critical state services continue despite interruption;
- DAS Enterprise Technology Services Customer Service Agreements document support provided to customers of the State network
- DAS has contracts with Internet Service Providers to provide network services to the State of Oregon.

Activation

Procedures in this annex will be implemented as outlined in the Oregon Emergency Operations Plan, Basic Plan.

When a major cyber incident emergency has occurred or credible information indicates that one is imminent, procedures in this annex may be automatically implemented under the following conditions:

- When determined necessary by DAS, OEM/OMD and the Governor.
- This annex identifies the major response and recovery activities undertaken by state and adjunct agencies in response to a cyber-incident

OEM has three levels of activation: Standby, Limited, and Full. The three levels of activation are described as follows:

Level I – Standby Activation

This is the lowest level of activation. The Duty officer receives a call through the Oregon Emergency Response System (OERS) Communications Center and tracks incidents. The on-call manager and appropriate state agencies are notified as necessary. This level of activation is maintained by the staffing of the OERS Communications Center on a 24-hour basis.

Level II – Limited Activation

A limited activation of the ECC occurs when a situation requires assistance from several state agencies. Its purpose is to coordinate the state's emergency response from a central location. OEM notifies the appropriate state agencies of a potential emergency or disaster and informs them a representative may be needed in the ECC. The ECC is staffed appropriately to ensure coverage is available to address the needs of the incident. Limited activation is considered when:

- OERS receives an alert from an official warning point or agency indicating an impending incident or emergency;
- A localized emergency escalates, adversely affecting a larger area or jurisdiction and exceeding local response capabilities;
- A geographically limited disaster requires a closely coordinated response by more than one state agency;
- The city or county fails to act (ORS 401.032(2)).

Level III – Full Activation

During a full activation, all appropriate ECC positions are filled in accordance with the Oregon State ECC Organization Chart (Figure 5-1). Representatives of the military, administrative services, transportation, environmental quality, and state police departments and the Oregon Health Authority represent a core group that is essential to handle most major emergencies. The situation may require the participation of other key agencies, depending on the nature of the incident. Full activation requires the ECC to be staffed on a 24-hour basis. Full activation is considered when:

- A localized emergency escalates, adversely affecting a larger area or jurisdiction and exceeding local response capabilities;
- OERS receives an alert from an official warning point or agency indicating a probable disaster or on a local level disaster or emergency.
- A Governor's 'State of Emergency' is issued.
- Terrorist or "weapons of mass destruction" activities are occurring or imminent.
- An alert, site-area emergency, or general emergency is declared at the Washington Nuclear Power Plant #2, Hanford reservation in Washington State, or research reactors at Oregon State University or Reed College.

4. Situation and Assumptions

The response to and recovery from a cyber-incident must take into account existing challenges to the effective management of significant cyber incidents and the resulting physical effects of such cyber incidents and of cyber consequences of physical incidents. Such consideration allows resources to be appropriately channeled into resolving identified challenges. Assumptions and identifiable challenges include but not limited to:

- National Incident Management System and National Response Framework are adaptable to cyber incidents.

- Management of Multiple Cyber Incidents: The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to adequately manage the cyber incident. Strategic planning and exercises should be conducted to assist in addressing this problem.

- Availability and Security of Communications: A debilitating infrastructure incident could impede communications needed for coordinating response and recovery efforts. Flexible secure, reliable communication systems are needed to enable public and private-sector entities to coordinate efforts in the event that routine communications channels are inoperable.
- Availability of Expertise and Surge Capacity: State and Federal agencies must ensure that sufficient technical expertise is developed and maintained within the Government to address the wide range of ongoing cyber incidents and investigations. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised, and maintained.

- Coordination with the Private Sector: Cyberspace is largely owned and operated by the private sector; therefore, the authority of the State and Federal Government to exert control over activities in cyberspace is limited.

5. Roles and Responsibilities

No single state agency will, in all cases, have the necessary resources or authority to carry out all response and recovery activities for an emergency or disaster. Therefore, coordination among agencies is essential. A Unified Command arising from a cyber-incident will be located in an Agency Operations Center (AOC) and/or the State Emergency Coordination Center (ECC). This recognizes that a cyber-incident may not occur in isolation. "Effective unified command is indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization. Success requires unity of effort, which respects the chain of command of each participating organization while harnessing seamless coordination across jurisdictions in support of common objectives."

State agencies are represented by their Emergency Support Functions (ESF) in the ECC during activation. Other state departments and agencies, not specifically designated under this annex, may have authorities, resources, capabilities, or expertise required to support operations. Agencies may be requested to participate in response and recovery operations, and may be asked to designate staff to function as liaison officers and provide other support.

Primary Agency – Department of Administrative Services (DAS):
A primary agency is an entity with significant authorities, roles, resources, or capabilities for functions defined within the Annex. When the Cyber Annex is activated in response to an incident, the primary agency is responsible for:

- Supporting the ESF coordinator and coordinating closely with the other primary and support agencies.

- Orchestrating support within their functional area for the State.

- Providing staff for the operations functions at fixed and field facilities.

- Notifying and requesting assistance from support agencies.

- Managing mission assignments and coordinating with support agencies, as well as appropriate State officials, operations centers, and agencies.

- Working with appropriate private-sector organizations to maximize use of all available resources.
- Supporting and keeping other ESFs and organizational elements informed of ESF operational priorities and activities.
- Conducting situational and periodic readiness assessments.
- Executing contracts and procuring goods and services as needed.
- Ensuring financial and property accountability for Cyber Annex activities.
- Planning for short- and long-term incident management and recovery operations.
- Maintaining trained personnel to support interagency emergency response and support teams.
- Identifying new equipment or capabilities required to prevent or respond to new or emerging threats and hazards, or to improve the ability to address existing threats.
- Coordinate with the United States Computer Emergency Response Team (US-CERT) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Analyzing cyber vulnerabilities, exploits, and attack methodologies.
- Providing technical assistance.
- Providing indications and warning of potential threats, incidents, and attacks.

Support Agencies

Support agencies are those entities with specific capabilities or resources that support the primary agency in executing the Cyber Annex mission. When the Annex is activated, support agencies are responsible for:

- Conducting operations, when requested by primary agency, consistent with their own authority and resources, except as directed otherwise pursuant to sections 402,403, and 502 of the Stafford Act.

- Participating in planning for short- and long-term incident management and recovery operations and the development of supporting operational plans, SOPs, checklists, or other job aids, in concert with existing first-responder standards.

- Assisting in the conduct of situational assessments.

- Furnishing available personnel, equipment, or other resource support as requested by primary agency.

- Providing input to periodic readiness assessments.

- Maintaining trained personnel to support interagency emergency response and support teams.

- Identifying new equipment or capabilities required to prevent or respond to new or emerging threats and hazards, or to improve the ability to address existing threats.
- Oregon Emergency Management:

- Will activate and staff the management structure of the State Emergency Coordination Center (ECC) as outlined in the Basic Plan of the State Emergency Operations Plan (EOP).

Emergency Coordination Center (ECC):

- The ECC is responsible for Oregon’s interagency emergency management and coordinating Federal and State Roles.

- Support agencies will assign personnel to the ECC.

- DAS, as the agency responsible for implementation of the Cyber Annex will respond directly to the Officer in Charge/Operations Officer in the State ECC. Alternatively, if the governor determines that the emergency is related to computer or telecommunication systems, he or she may designate the department of administration as the lead agency to respond to that emergency.

- Oregon Emergency Management and DAS may assign lead coordinating responsibilities to the appropriate agencies based on the physical impact of a cyber-incident.

- The ECC will be responsible for coordination with the US DHS Unified Coordination Group (UCG) or other Federal Incident Response organizations.

- ECC operations will be tailored with personnel and materials from State Agencies in response to the cyber incident. DAS provides subject-matter expertise related to the cyber threat, analysis, and recommendations to the ECC. The ECC will be activated at one of the levels as described above under “Activation.”

Fusion Center:
Fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal and state, local, tribal, territorial and private sector partners.

6. Concept of Operations

General

DAS, the primary agency, plays a significant role in managing intergovernmental (Federal, State, local, and tribal) and, where appropriate, public-private coordination in response to a cyber-incident. Responsibilities include:

- Providing indications and warning of potential threats, incidents, and attacks;

- Information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation;

- Analyzing cyber-vulnerabilities, exploits, and attack methodologies;

- Providing technical assistance;

- Conducting investigations and forensics analysis;

- Defending against the attack; and

- Leading national-level recovery efforts.

These activities are the product of, and require, a concerted effort by Federal, State, local, and tribal governments, and nongovernmental entities such as private industry and academia.

Not all national level cyber incidents will have statewide significance. Likewise a statewide incident may not have national significance. Statewide cyber emergencies may include:

- Cyber incidents determined to be severe enough to be a declaration by the Governor under the provisions of ORS 401.165 .

- Cyber incidents either intentional or unintentional, which threatens Oregon's economic prosperity through a loss of confidentiality, integrity, or availability of the communications, data or information infrastructure.

7. Direction and Control

Notification of a cyber-incident will be initiated by the primary agency. Upon notification, the Oregon Emergency Coordination Center (ECC) will be alerted at a level determined by DAS and OEM
Following notification the following actions will be taken:

- DAS will establish the facts and assumptions concerning the cyber incident. This will require establishing a single liaison with private sector entities involved in the restoration of services after an incident occurs. Private sector entities will be consulted in the cyber response decision making processes.

- Following establishment of initial facts concerning the incident the ECC in conjunction with DAS:
  - Recommend the ECC operating level.
  - Seek assistance from and/or provide recommendations to impacted agencies.

- The ECC and DAS will cooperatively assess the on-going impacts of the incident, provides analysis of the extent and duration of incident, and identifies requirements for consequence management.

- In coordination with impacted agencies and jurisdictions, DAS will recommend prioritization of actions for the restoration of computer and network services during response and recovery operations.

During a significant incident, DAS may report incident information to external organizations. Reports will contain an appropriate classification based on the type of incident and clearance by the ECC. Recipients shall agree to observe the classification.

8. Supporting Plans and Procedures

To Be Developed

9. Appendices

- Appendix A Glossary

Appendix A – Glossary

Agency Operations Center (AOC) - The location or locations from which individual state agencies control their resources and operations. Most state agencies have a single AOC, some have several regional AOCs

Emergency Coordination Center (ECC) - The State ECC is the single point of contact for an integrated state response to an emergency. The purpose of the ECC is to provide a centralized location where state officials may coordinate activities and implement direction from the Governor. The primary responsibility of the ECC is to provide information, policy direction and coordination for a major emergency or disaster. This is achieved through a unified management approach.

Emergency Operations Plan (EOP) - A document that: describes how people and property will be protected in disaster and disaster threat situations; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available for use in the disaster; and outlines how all actions will be coordinated.

Emergency Support Function (ESF) – A functional area of response activity established to facilitate the delivery of Federal assistance required during the immediate response phase of a disaster to save lives, protect property and public health, and to maintain public safety. ESF represent those types of federal assistance that the State would most likely need because of the overwhelming impact of a catastrophic or significant disaster on its own resources and response capabilities or because of the specialized or unique nature of the assistance required. ESF missions are designated to supplement state and local response efforts.

Fusion Center - Fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal and state, local, tribal, territorial and private sector partners.

National Incident Management System (NIMS) A system mandated by HSPD-5 that provides a consistent, nationwide approach for federal, state, local, and tribal governments; the private-sector; and Non-Governmental Organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents regardless of cause, size, or complexity. To provide for interoperability and compatibility among federal, state, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the Incident Command System (ICS); multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

National Response Framework (NRF) - A guide to how the Nation conducts all-hazards incident management. It is built upon flexible, scalable, and adaptable coordinating structures to align key roles and responsibilities across the Nation. It is intended to capture specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. The National Response Framework replaces the former National Response Plan.

Oregon Emergency Response System (OERS) - OERS is a service provided 24 hours a day as prescribed by ORS 401.275. OERS provides a coordinated state and federal response to incidents involving chemicals, petroleum products, biological agents, radioactive materials, and other technological and natural hazards. OERS is the point of contact for initiating state assistance in Search and Rescue activities. It is the only telephone number that local agencies need to call in order to notify the appropriate state and federal agencies (1-800-452-0311 or (503) 378-6377). OERS activities are governed by the OERS Council[1].

Primary Agency - This position is filled only during disasters involving the activation of the National Response Framework. The Primary State Agency coordinates the activities of their State of Oregon Support Function (SSF) with the Federal counterparts in the designated Emergency Support Function (ESF).

State Incident Response Team (SIRT) - The State Incident Response Team responds to information security incidents that potentially impact multiple agencies or which pose a significant threat to the State of Oregon. The SIRT is responsible for coordinating interagency security incident response resources and communications during or about an information security incident that impacts multiple agencies.

Support Agencies - Within the State ECC, support agencies provide resources and staffing that contribute to the overall accomplishment of the mission of the State Support Function. Not every Support

Agency will have input to, or responsibilities for, the accomplishment of every mission assigned to the State Support Function.

[1] ORS 401.054 describes the designated support agencies and liaisons to the state ECC. Pursuant to SB-33(2013-Legislative Session), currently (05/31/2013) before the Joint Ways and Means Committee….