ESF 17 — Cyber and Infrastructure Security

Purpose

Emergency Support Function (ESF) 17 is 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.

Coordinating Agencies

PRIMARY AGENCY: Clackamas County Technology Services (TS)
SUPPORTING AGENCY: Clackamas County Sheriff's Office (CCSO), Clackamas County Disaster Management (CCDM); Risk Management

Scope

In the event of a significant cybersecurity incident, ESF 17 provides a centralized entity for responding to a cyber incident that affects Clackamas County. ESF 17 provides a means of defining, specifying, and maintaining the functions and resources required to ensure timely and consistent actions, communications, and response efforts.

Additionally, ESF 17 ensures appropriate coordination and inclusion of necessary state, federal, local agencies and private agencies, in order to minimize the impact of a cybersecurity incident. Significant cybersecurity incidents may occur independently or in conjunction with disaster emergency operations and potentially could impact public health, safety, or critical infrastructure.

ESF 17 stakeholders coordinate in accordance with relevant statutory and regulatory authorities during all phases of emergency management. ESF 17 stakeholders coordinate with state and local departments and agencies during response, but do not supersede the authority of these entities. ESF 17 and relevant state and local entities work together to protect life and property in the State of Oregon.

Response

Response activities take place **during** an emergency and include actions taken to save lives and prevent further property damage in an emergency situation.

Response roles and responsibilities for ESF 17 include:

Technology Services

- ❑ Detect and triage potential cyber incidents
- ❑ Develop and coordinate threat alerts and critical bulletins
- ❑ Analyze the event and articulate potential impacts to relevant stakeholders and state leadership
- ❑ Document facts, gather and maintain evidence as needed to support criminal investigations, coordinating with the affected entity for key threat indicators
- ❑ Schedule an initial conference with the affected entity to assess the incident, classify its severity on the severity matrix, determine Lead entity within CISO and the parties needed to support the Initial Response Team (IRT), and activate the IRT
- ❑ Activate and execute pertinent response plans
- ❑ Notify the SOC of any changes to the incident severity level
- ❑ Provide regular briefings or updates to elected officials and/or department leadership
- ❑ Deploy tactics to contain, eradicate, and recover from a cyber incident
- ❑ Ensure confidentiality, integrity, and availability of all information related to the incident
- ❑ Report incidents using proper incident handling or notification protocols to all relevant local, County, state, federal, and commercial entities as outlined in the JCIRG

Disaster Management

- ❑ Activate the Emergency Operations Center
- ❑ Advise the County Administrator and BCC.
- ❑ Facilitate the Emergency Declaration process.
- ❑ Coordinate with city, regional, and State counterparts.
- ❑ Assist in multi-agency/multi-jurisdictional and resource coordination.

CCSO

- ❑ Sheriff or designee: participate in EOC Command representing law enforcement Countywide.
- ❑ Provide law enforcement personnel to staff EOC positions.
- ❑ Coordinate law enforcement response activities.
- ❑ Analyze law enforcement resource needs and request assistance through the EOC.
- ❑ Work within NIMS/ ICS/EOC JIC to provide public information.

EOC Operations

When cyber and infrastructure security activities are staffed in the EOC, the TS representative will be responsible for the following:

- Serve as a liaison with supporting agencies and community partners.
- Provide a primary entry point for situational information related to cyber and infrastructure security.
- Share situation status updates related to cyber and infrastructure security to inform development of Situation Reports.
- Participate in and provide cyber and infrastructure security-specific reports for EOC briefings.
- Assist in development and communication of cyber and infrastructure security-related actions to tasked agencies.
- Monitor ongoing cyber and infrastructure security-related actions.
- Share cyber and infrastructure security-related information with the Public Information Officer (PIO) to ensure consistent public messaging.
- Coordinate cyber and infrastructure security-related staffing to ensure the function can be staffed across operational periods.

Coordinating with Other ESFs

The following ESFs support ESF 17-related activities:

- **ESF 1 – Transportation.** Assist in transportation of investigation personnel to impacted areas, and assist necessary logistical workflow.
- **ESF 2 – Communications.** Augment communications resources to County, local, state, and federal agencies.
- **ESF 13– Law Enforcement.** Provide support for law enforcement resources, investigations, and reports.

Preparedness

Preparedness activities take place **before** an emergency occurs and include plans or preparations made to save lives and to help response and recovery operations.

Preparedness roles and responsibilities for ESF 17 include:

Technology Services

- ❑ Maintain the ESF 17 Annex and support an iterative and collaborative planning process
- ❑ Build the state's capacity to collectively respond to cyber incidents:
- ❑ Conduct and/or participate in cybersecurity awareness training and exercises, in coordination with OR Cyber Security Advisory Council to increase awareness about cyber hygiene and best practices
- ❑ Conduct and/or participate in cybersecurity training and exercises to continuously validate planning concepts and operations.
- ❑ Establish and maintain working relationships with local, County, state, and federal entities to support the improvement of state response capabilities and improve coordination
- ❑ Monitor information and potential threats using multiple information pathways (e.g., Open-Source Intelligence [OSINT], coordination with fusion centers)
- ❑ Conduct cyclical analysis of risk to assess and achieve operational benchmarks
- ❑ Develop and revise incident handling and reporting plans, protocols, and policies on a continuous basis, and subsequently publicize those changes with relevant audiences
- ❑ Identify resources to support incident preparedness, response, and recovery and training stakeholders on available resources
- ❑ Maintain and train the IRT
- ❑ Maintain and update all local, County, state, federal, and commercial contact lists and test contact methods on at least a quarterly basis
- ❑ Maintain relationships and contact information for all other ESFs.

Mitigation

Mitigation activities take place **before and after** an emergency occurs and includes activities that prevent an emergency, reduce the chance of an emergency happening, or reduce the damaging effects of unavoidable emergencies.

Mitigation roles and responsibilities for ESF 17 include:

All Tasked Agencies:

- ❑ Participate in the hazard/vulnerability identification and analysis process.
- ❑ Take steps towards correcting deficiencies identified
- ❑ During the hazard/vulnerability identification and analysis process as appropriate.

Mitigation

Technology Services

- ❑ Oversee the implementation of processes to mitigate the impacts of cyber-incidents, including but not limited to:
  - ❑ Performing recurring data backup
  - ❑ Maintaining off-site data storage
  - ❑ Maintaining awareness of alternate facilities and Point of Contact information
  - ❑ Performing security device configuration reviews
  - ❑ Continuously reviewing state networks and services policies and procedures

Recovery

Recovery activities take place **after** an emergency occurs and include actions to return to a normal or an even safer situation following an emergency.

Recovery roles and responsibilities for ESF 17 include:

All Tasked Agencies:

- ❑ Perform after-action analysis, develop an after-action report, and address corrective action items
- ❑ Participate in after action analysis conducted by the state and other ESFs upon request
- ❑ Support damage assessments, as needed.

ESF 17– Cyber and Infrastructure Security

(Working Draft: Developed November 2021)

THIS PAGE LEFT BLANK INTENTIONALLY

Table of Contents

THIS PAGE LEFT BLANK INTENTIONALLY

ESF 17 Tasked Agencies	
Primary County Agency	Clackamas County Technology Services (TS)
Supporting County Agency	Clackamas County Sheriff's Office (CCSO), Clackamas County Disaster Management (CCDM), Risk Management
Community Partners	None at this time
State Agency	Oregon Office of Emergency Management (OEM)
Federal Agency	Federal Bureau of Investigations (FBI)

1 Introduction

1.1 Purpose

Emergency Support Function (ESF) 17 is 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.

This Annex will facilitate, coordinate, and support the following core functions of the ESF:

- Refining inter-agency and cross-sector information coordination, encouraging information sharing, and performing threat analysis;
- Sharing information in a way that protects privacy, confidentiality, and civil liberties;
- Establishing and maintaining the Incident Response Team (IRT) to detect, report, and respond to cyber incidents; and
- Developing a statewide cybersecurity strategy that advances Oregon's cyber capabilities.

1.2 Scope

In the event of a significant cybersecurity incident, ESF 17 provides a centralized entity for responding to a cyber-incident that affects Clackamas County. ESF 17 provides a means of defining, specifying, and maintaining the functions and resources required to ensure timely and consistent actions, communications, and response efforts. Additionally, ESF 17 ensures appropriate coordination and inclusion of necessary state, federal, local agencies and private agencies, in order to minimize the impact of a cybersecurity incident. Significant cybersecurity incidents may occur independently or in conjunction with disaster emergency operations and potentially could impact public health, safety, or critical infrastructure.

ESF 17 stakeholders coordinate in accordance with relevant statutory and regulatory authorities during all phases of emergency management. ESF 17 stakeholders coordinate with state and local departments and agencies during response, but do not supersede the authority of these entities. ESF 17 and relevant state and local entities work together to protect life and property in the State of Oregon.

1.3 Policies and Agreements

The Oregon State Legislature set forth policies in Chapter 276A – Information Technology. Below are Oregon Revised Statutes (ORS) that are particularly relevant to cyber and infrastructure security:

- ORS 276A.300
- ORS 276A.303
- ORS 276A.306
- ORS 276A.323
- ORS 276A.326
- ORS 276A.329
- ORS 276A.332
- ORS 276A.335

2 Situation and Assumptions

2.1 Situation and Assumptions

The response to and recovery from a cyber-incident must consider 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:

- 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.

3 Concept of Operations

3.1 General

The Department of Administrative Services (DAS) is the primary agency that plays a significant role in managing intergovernmental (Federal, State, Local, and Tribal) and, where appropriate, public-private coordination in response to cyber-incident. Responsibilities including:

- 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;
- Leading county-level recovery efforts.

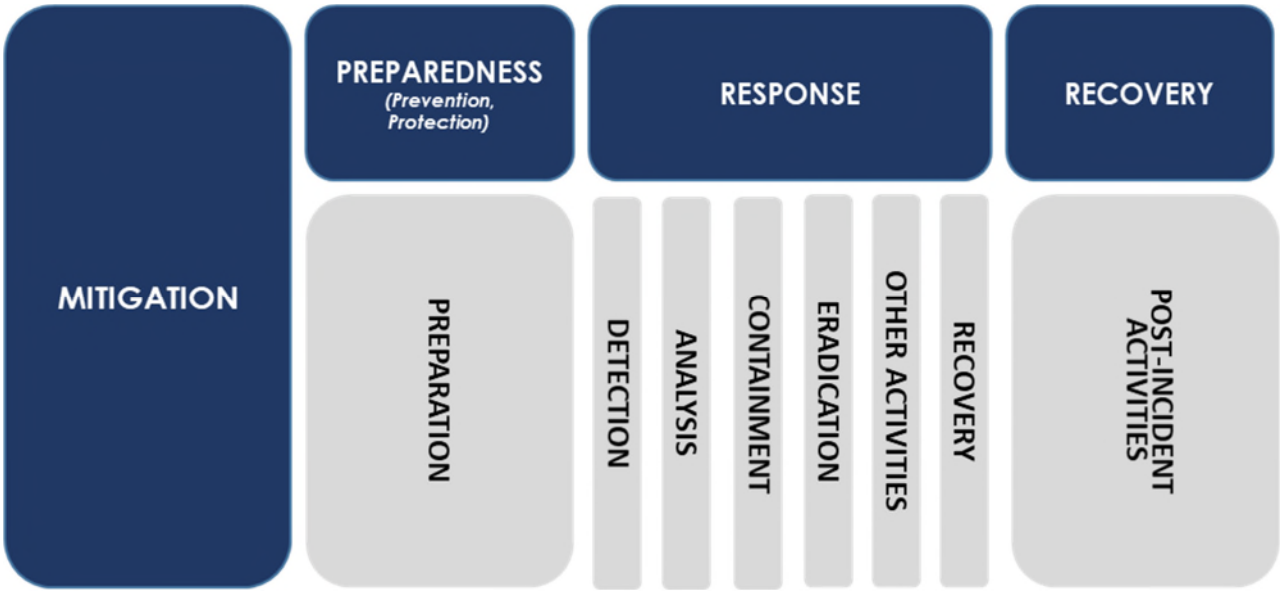
These activities are the product of, and require, a concerted effort by Federal, State, local, and tribal governments, and nongovernmental entities such as private industry and academia. Not all national level cyber incidents will have statewide significance. A statewide incident may not have national 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.

3.2 Cyber Incident Management Phases

Cyber incidents require the involvement of both information technology experts and emergency management. To provide clarity to all sides of the multi-faceted response partners, the following matrix (Figure Pictured Below) depicts the overlap between emergency management activities and information technology activities, using terminology familiar to each set of stakeholders.

Figure 17-1. Cyber-Incident Management Process in Relation to Emergency Management Phases



3.3 Incident Response Team

The Incident Response Team (IRT) can be established and facilitated by local, state, and federal agencies. During the initial conference between the affected entity, the Chief Information Security Officer will appoint team members as needed.

Upon activation, the IRT will be responsible for:

- Implementing tactical response operations to detect, analyze, contain, eradicate, and recover from an incident within their respective line(s) of effort
- Receiving strategic direction and guidance from governing authorities and aligning response actions appropriately
- Coordinating with public and private sector entities within the state to implement proper threat detection, reporting, and response procedures
- Establishing a regular reporting schedule to provide updates to governing authorities to create and maintain situational awareness and support operational coordination and coordinating with Emergency Operations Command to:
    - Conduct briefings or share information with non-state partners
    - Provide recurring reporting to Federal entities using designated reporting procedures to meet regulatory requirements, and create and maintain situational awareness at the federal level
- Providing support to law enforcement agencies responsible for criminal investigation during cyber incidents and state agencies responsible for advancing information security
- Facilitating the collection and proper handling of evidence
- Providing technical support to the affected entity to facilitate cyber incident resolution

3.4 Cyber Incident Response Lines of Effort

As described in Table 17-1 below, there are four lines of effort in cyber incident response: Threat Response, Asset Response, Intelligence Support, and Affected Entity Response. These concurrent lines of effort provide the foundation required to synchronize various response efforts before, during, and after a cyber incident, as defined below.

Table 17-1. Cyber Incident Response Lines of Effort, Defined

Line of Effort	Definition
Threat Response	Activities include the appropriate law enforcement investigativeactivities for: • Collecting evidence and gathering intelligence to provideattribution • Linking related incidents and identifying additional possibleaffected entities • Identifying threat pursuit and disruption opportunities • Developing and executing courses of action to mitigate theimmediate threat and facilitating information sharing and coordination with Asset Response efforts
Asset Response	Activities include furnishing technical assistance to affectedentities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents by: • Identifying other entities possibly at risk and assessing their riskto the same or similar vulnerabilities • Assessing potential risks to the sector or region, includingpotential cascading effects, and developing courses ofaction to mitigate these risks • Facilitating information sharing and operational coordinationwith Threat Response • Providing guidance on how best to utilize state and local resources and capabilities in a timely, effective manner tospeed recovery

Intelligence Support	Facilitates the building of situational threat awareness andsharing of related intelligence to: • Create an integrated analysis of threat trends and events • Identify and assist with the mitigation of knowledge gaps • Suggest methods to degrade or mitigate adversary threatcapabilities
Affected Entity Response	• Highly encouraged to share information surrounding the event with other cybersecurity specialists to assist with the investigative, analysis, response, and recovery phases of cyber incident response • The affected entity is the data owner and retains responsibilities to ensure appropriate actions and safeguards are in place to remediate threats and secure their information

3.5 Coordination with Other ESFs

The following ESFs support ESF 17-related activities:

- **ESF 1 – Transportation.** Assist in transportation of investigation personnel to impacted areas, and assist necessary logistical workflow.
- **ESF 2 – Communications.** Augment communications resources to county, local, state, and federal agencies.
- **ESF 13 – Law Enforcement.** Provide support for law enforcement resources, investigations, and reports.

4 Emergency Coordination

Clackamas County ESF 17 coordinates across a diverse group of stakeholders and entities, with the Clackamas County Chief Information Security Officer (CISO) serving in a role to facilitate information and resource sharing among ESF partners.CISO facilitates cyber coordination among state, local, and federal governmental partners, emergency management, State Threat Assessment Center (STAC), and Regional Fusion Centers (RFCs). While Clackamas County CISO has a formal role in coordinating with federal partners, state and local emergency management, and the STAC, its role in coordination with RFCs is based on requests for support and information sharing.

Regional Fusion Centers request state support for cyber-driven incidents through Clackamas County CISO, as stipulated by Oregon State law. Beyond this relationship, RFCs can also look to Clackamas County CISO as a resource for information and resources that may be needed to respond to and recoverfrom a cyber-incident.

CISO's connections with diverse cyber, law enforcement, and emergency management partners allow it to act as a conduit of needed intelligence, equipment,expertise, and staff between partners. In this way, ESF 17 coordinates through the Clackamas County CISO as the main resource for information and resources during a cyber-incident involving response from Clackamas County ESF 17 partners.

4.1 Regional, State, and Federal Assistance

Successful operation of the Clackamas County ESF 17 requires coordination with a diverse group of stakeholders, including regional partners. Regional Fusion Centers (RFCs) in particular, play a key role in cyber incident response at the regional level. Fusion centers provide valuable intelligence and response capabilities that can contribute to the mission of ESF 17.

4.1.1 Fusion Center Responsibilities

As a key member of Clackamas County ESF 17, a primary responsibility for RFCs is to provide situational awareness on incidents to the Chief Information Security Officer (CISO). These fusion centers can provide situational awareness updates to CISO even when they are not requesting support from state entities. This one-way communication allows CISO to remain aware of ongoing threats and provide expeditious support when requested. Fusion centers may also request state-level incident response support from CISO, including support for information and resource sharing. When support is requested, CISO can leverage state resources as well as connect regional entities to other actors with a given set of specialized skills or resources.

4.1.2 Tertiary Response Support

Clackamas County CISO may support response to cyber incidents occurring within non-state entities, if requested, and resources are available to support. The following conditions and actions are associated with assistance to non-state entities.

- Monitor the status of the external, non-state entity's cyber incident throughoutthe event lifecycle
- Provide Clackamas County and state leadership periodic updates on the external, non-State entity's cyber incident and whether any aspects of it are\can\may adversely affect Oregon digital technologies, systems, operations, or services
- Initiate the recommendation for IRT stand up if the external, non-state entity's cyber incident reaches a point where it adversely affects Oregon digital technologies, systems, operations, or services up to Level 2 (Medium) or higher

5 ESF Annex Development and Maintenance

The Technology Services Department will be responsible for coordinating regular review and maintenance of this annex. Each primary and supporting agency will be responsible for developing plans and procedures that address assigned tasks.

6 Appendices

Appendix A. Cyber-Incident Severity Matrix

Oregon Cyber Incident Severity	Description	Level of Effort Description of Actions
Level 0—Steady State	Unsubstantiated or inconsequential event.	Steady State, which includes routine watch and warning activities.
Level 1—Low	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties,or public confidence.	Requires coordination among State Departments and SLTT governmentsdue to minor to average levels andbreadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.
Level 2—Medium	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or publicconfidence.	Requires coordination among Victim Departments, Victim Agencies, or SLTT governments dueto minor to average levels and breadth of cyber related impact ordamage. Typically, this is primarily a recovery effort.
Level 3—High	Likely to result in a demonstrable impact to publichealth or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments dueto moderate levels and breadth ofdamage. Potential involvement of FEMA and other federal agencies.
Level 4—Severe	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Requires elevated coordination among State Departments, State Agencies, or SLTT governments dueto moderate levels and breadth ofcyber impact or damage. Involvement of Federal Partners if needed for incident.
Level 5—Emergency	Poses an imminent threat to the provision of wide scale critical infrastructure services,State government security, orthe lives of Oregon citizens.	Due to its severity, size, location, actual or potential impact on public health, welfare, or infrastructure, the cyber incident requires an extreme amount of State assistance for incident response and recovery efforts, for which the capabilities to support do not exist at any level of State government. Involvement of Public Private Partnerships if needed for incident.