ESF 17 – Cyber and Critical Infrastructure Security

LAST UPDATED: 20 April 2022

THIS PAGE LEFT BLANK INTENTIONALLY

ESF 17 – Table of Contents

THIS PAGE LEFT BLANK INTENTIONALLY

ESF 17 Tasked Agencies	
Primary Agencies	Oregon TITAN Fusion Center DAS – EIS (Cyber Security Services)
Supporting Agencies	Oregon Office of Emergency Management (OEM) Oregon State Police (OSP)
Adjunct Agency	Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA)

1 Introduction

1.1 Purpose

Emergency Support Function (ESF) 17 describes how the State of Oregon will coordinate plans, procedures and resources to support the state's response to protect cyber and critical infrastructure and key resources threatened by human or natural caused emergencies. Critical infrastructure and key resources are the 16 critical infrastructure sectors whose assets, systems and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety or any combination thereof.

1.2 Scope

Activities encompassed within the scope of ESF 17 include:

- Establishing procedures for the use of other state and federal resources (to include Oregon National Guard) in public safety and security missions requested by local authority having jurisdiction.
- Coordinating pre-incident management planning and actions to assist in the prevention or mitigation of threats and hazards. This includes the development of operational and tactical plans, the conducting of technical security and/or vulnerability assessments and deployment of state public safety and security resources in response to specific threats for potential incidents.
- Preparing and maintaining state infrastructure and capabilities through coordination, training and exercises.
- Providing technical assistance related to security planning efforts and conducting technical assessments (e.g., vulnerability assessments, risk analyses).
- Maintaining availability of resources and how to request them.

1.3 Related Functions

ESF 17 often works closely with other State ESFs as a part of coordinated response and recovery activities. The following ESFs support cyber and critical infrastructure-related activities:

- **ESF 2 – Communications.** Support interoperable communications and access to communications infrastructure.
- **ESF 12 – Energy.** Regulatory responsibility for Energy Sector and access to external resources.
- **ESF 13 – Law Enforcement**. Oregon TITAN Fusion Center operations, criminal investigation support, supplement local law enforcement for security needs.
- **ESF 15 – Public Information.** Message key information to the public.
- **ESF 18 – Military Support.** Augment civilian law enforcement operations as needed.

2 Situation and Assumptions

2.1 Situation

Oregon is faced with a number of hazards that may result in impacts to cyber and critical infrastructure. Considerations that should be taken into account when planning for and implementing ESF 17 activities include:

- Significant disasters and emergency situations have the ability to damage infrastructure and lifelines that can overwhelm local abilities.
- A cyber incident is a single or series of unwanted or unexpected security events that results in harm, or poses a significant threat of harm, to information assets, an agency, or third party and requires non-routine preventive or corrective action.
- A cyber event is an observable, measurable occurrence involving an information asset that is relevant to security operations.
- Cyber threats reaching an emergency declaration
- National Level1/Level2 Critical Infrastructure is severely degraded
- An event that causes cascading impacts either as a result or otherwise will require coordination between state, local, tribal and federal entities

2.2 Assumptions

ESF 17 is based on the following planning assumptions:

- The availability of resources will have a profound effect on agencies' abilities to perform tasked activities
- Timeliness of reporting impacts to response
- Events that cause large-scale impacts to cyber and critical infrastructure will likely require assistance from federal partners
- In the event of potential community or sensitive informational impacts, notification will be necessary
- Impacts with the potential for a significant impact to national security are confidential and will be coordinated with federal partners
- Emerging real and perceived cyber threats can cause undue fear and concern that can impact response

3 Roles and Responsibilities

The following section outlines the roles and responsibilities assigned to state agencies and community partners to ensure ESF 17 activities are performed in an efficient and effective manner to support response and recovery. This document does not relieve tasked agencies with the responsibility for emergency planning, and agency plans should adequately provide for the capability to implement the actions identified below.

3.1 Primary Agencies

The primary agencies for ESF 17 are the Oregon TITAN Fusion Center (OTFC) and DAS – EIS. These agencies are responsible for the following overarching coordination activities:

- Coordinating regular review and update of the ESF 17 annex with supporting agencies
- Facilitating collaborative planning to ensure state capability to support ESF 17 activities
- Providing a representative to the State ECC, when requested, to support ESF 17 activities
- Managing mission assignments and coordinating with support agencies, as well as appropriate State officials, operations centers and agencies

- Supporting and keeping other ESFs and organizational elements informed of ESF operational priorities and activities
- Facilitating transition to recovery

3.1.1 Oregon TITAN Fusion Center (OTFC)

OTFC is responsible for information sharing between local, state and federal partners to better communications to support the prevention, response and disruption of threats to Oregon. Key ESF 17 responsibilities for the OTFC include:

- Facilitating the Critical Infrastructure and Key Resources (CIKR) Program
- Developing and maintaining a liaison between local, state and federal law enforcement agencies in Oregon, assisting them in the investigation and suppression of organized criminal activity and encouraging cooperation among those agencies.
- Establishing a coordinated system of collecting, storing and disseminating information relating to infrastructure protection
- Conducting comprehensive factual studies of organized criminal activity in Oregon, outlining existing state and local policies and procedures with respect to organized crime and formulating and proposing such changes in those policies and procedures as the Department may deem appropriate.
- Notify partners of incidents as appropriate and relevant.

3.1.2 EIS Cyber Security Services

EIS Cyber Security Services is responsible for enterprise security policy, security monitoring of the state network, enterprise incident response and enterprise security architecture, as well as dissemination of security training, policy and best practices across state government (Executive Branch only). Key ESF 17 responsibilities for EIS include:

- Providing staff for the operations functions at fixed and field facilities
- Working with appropriate private-sector organizations to maximize use of all available resources
- Executing contracts and procuring goods and services as needed
- 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
- Coordinating with CISA and the Multi-State Information Sharing and Analysis Center and additional federal partners
- Analyzing cyber vulnerabilities, exploits and attack methodologies
- Providing indications and warning of potential threats, incidents and attacks
- Make recommendations regarding additional cyber infrastructure partners

3.2 Supporting Agencies

Supporting agencies contribute to the overall accomplishment of the mission of the ESF. Not every support agency will have input to or responsibility for, the accomplishment of every mission assigned to the ESF.

3.2.1 Oregon State Police

OSP is Oregon's primary law enforcement agency and is tasked with protecting the people, property and natural resources of the state. Key ESF 17 responsibilities for OSP include:

- Developing and maintaining a liaison between local, state and federal law enforcement agencies in Oregon, assisting them in the investigation and suppression of organized criminal activity and encouraging cooperation among those agencies.
- Acting as an initial incident command agency until the local incident command agency is on-scene or if no local agency is available.
- Providing limited damage assessment as their duties permit.
- Providing for the protection of life and property, traffic control, crowd control, communications, emergency first aid, site security and security for vital state facilities and critical infrastructure. Generally, law enforcement within the disaster/emergency area remains the responsibility of local authorities along established jurisdictional boundaries, unless state assistance is requested or required by statute.
- Personnel assigned to the Counter Terrorism Section (CTS) participate in active investigations of international and domestic terrorism, coordination of similar federal and local investigations, involvement in domestic preparedness issues and intelligence matters.

- Oregon Emergency Response System (OERS): OERS is the primary point of contact by which any public agency provides the state notification of an emergency or disaster or requests access to state or federal resources. OERS provides a 24-hour service.

- Criminal Justice Information System (CJIS)/Law Enforcement Data System (LEDS) is the focal point and "control agency" for access by law enforcement and criminal justice agencies in Oregon to the online information in the Federal Bureau of Investigations (FBI) National Crime Information Center (NCIC), the interstate law enforcement message switching network and the National Law Enforcement Telecommunications System (NLETS), which is operated by a consortium of states. Since CJIS/LEDS computer terminals are located statewide in all law enforcement agencies and most public safety agencies, the system is used to relay critical public safety information both day-to-day and during disasters.

3.2.2 Oregon Office of Emergency Management

OEM is statutorily responsible for coordination of the state's emergency management program. Key ESF 17 responsibilities for OEM include:

- Providing a liaison, if needed, to assist in coordination of ESF 17 in the State ECC and at a FEMA Joint Field Office, if applicable.

- Expand, refine, and train partners in ECC operations to meet emerging and changing needs.

- Coordinating resource requests and emergency declarations.

3.3 Adjunct Agencies

Adjunct agencies are organizations that may not be part of state government but have direct role in the function.

3.3.1 Adjunct Agencies

- Department of Homeland Security - Cybersecurity and Infrastructure Security Agency

- Oregon and Region X Information Sharing and Analysis Centers

4 Concept of Operations

4.1 General

The State of Oregon Emergency Operations Plan, including ESF 17, is developed under the authority of Oregon Revised Statutes Chapter 401 which assigns responsibility for the emergency services system within the State of Oregon to the Governor (ORS 401.035). The Governor has delegated the responsibility for

coordination of the state's emergency program, including coordination of recovery planning activities to the Oregon Military Department, Office of Emergency Management (OEM; ORS 401.052). OEM, in turn, has assigned responsibility for coordination of the implementation of ESF 17 to the primary and supporting agencies identified above.

Additionally, Executive Order (EO)-16-07 establishes a Disaster Management Framework to facilitate Oregon's response and recovery actions and provides a flexible instrument for execution of prudent policy and decision-making. The EO establishes the Governor's Disaster Cabinet and Economic Recovery Councils that will serve as the policy making body during a large scale or catastrophic disaster in Oregon.

All ESF 17 activities will be performed in a manner that is consistent with the National Incident Management System and the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

4.2 Activation

When a disaster occurs, the OEM Executive Duty Officer may, based on the size and complexity of the situation, activate the State ECC and assume the role of ECC Manager. The ECC Manager will establish communications with leadership and gather situational information to determine an ECC staffing plan and set up operational periods. If the incident requires significant coordination of cyber and critical infrastructure protection activities, the ECC Manager may activate ESF 17. ESF 17 will report to the ECC Manager or the Coordination Section Chief (Infrastructure Branch) if activated. Upon ESF activation, notification will be made to the ESF primary agencies, OTFC and EIS-CSS. OTFC and EIS-CSS will coordinate with supporting agencies to assess and report current capabilities to the ECC and activate Agency Operations Centers as appropriate. Primary and supporting agencies may be requested to send a representative to staff the ECC and facilitate ESF 17 activities.

4.3 ECC Operations

When ESF 17 is staffed in the ECC, the ESF representative will be responsible for the following:

- Serving as a liaison with supporting agencies and partners
- Providing a primary entry point for situational information related to cyber and critical infrastructure needs
- Sharing situation status updates related to cyber and critical infrastructure with ESF 5, Information and Planning, to inform development of the Situation Report
- Participating in and providing ESF-specific reports for, ECC briefings including Disaster Cabinet and Economic Recovery briefings

- Assisting in development and communication of ESF 17 mission assignments to tasked agencies
- Monitoring ongoing ESF 17 mission assignments
- Sharing ESF 17 information with ESF 15, Public Information, to ensure consistent public messaging
- Coordinating ESF 17 staffing to ensure the function can be staffed across operational periods

4.4 Transition to Recovery

Intermediate and long-term recovery activities are guided by the State of Oregon Recovery Plan. In the event of a large-scale or catastrophic incident, the Governor may appoint a State Disaster Recovery Coordinator (SDRC) to facilitate state recovery activities and the longer-term aspects of cyber and critical infrastructure protection and coordination may be tasked to State Recovery Function (SRF) 6. The SDRC and the State Coordinating Officer (SCO) are responsible for agreeing on the timing of transition from response (ESF 17) to recovery (SRF 6).

See the Oregon State Recovery Plan, SRF 6, Infrastructure Systems, for additional information.

5 ESF Development and Maintenance

OTFC and EIS - CSS will be responsible for coordinating regular review and maintenance of this ESF Annex. Each primary and supporting agency will be responsible for developing plans and procedures that address assigned tasks. Final draft revisions will be sent to OEM for integration into the state Emergency Operations Plan.

6 Appendices

- Appendix A – ESF 17 Resources

Appendix A ESF 17 Resources

State

- State of Oregon Emergency Operations Plan
  - Incident Annex – Cyber Security
  - Support Annex – Critical Infrastructure and Key Resources
- State of Oregon Recovery Plan
  - SRF 6
- Oregon Revised Statutes
  - ORS 401
  - ORS 276A.300
- OTFC Plans and Procedures
  - Oregon State Infrastructure Protection Plan
- EIS – CSS Plans and Procedures
  - Statewide Incident Response Plan
  - Cyber Disruption Plan

Federal

- National Response Framework
  - ESF 13 – Public Safety and Security
- National Disaster Recovery Framework
- CISA
  - National Cyber Incident Response Plan
  - National Infrastructure Protection Plan