ESF 17:
Cyber and Infrastructure Security

THIS PAGE LEFT BLANK INTENTIONALLY

Table of Contents

ESF 17 Tasked Agencies	
Primary County Agency	Clackamas County Technology Services (TS) Clackamas County Finance Department – Facilities Management
Supporting Agencies	Clackamas County Sheriff's Office (CCSO) Clackamas County Disaster Management (CCDM) Risk Management Public and Government Affairs (PGA)
Community Partners	Local law enforcement agencies
State Agency	Oregon Department of Justice – TITAN Fusion Center Oregon Department of Administrative Services – Enterprise Information Services (EIS)
Federal Agency	Federal Bureau of Investigation (FBI) Department of Homeland Security - Cybersecurity and Infrastructure Security Agency (CISA)

THIS PAGE LEFT BLANK INTENTIONALLY

1 Introduction

1.1 Purpose

The Cybersecurity and Infrastructure Security Emergency Support Function (ESF-17) ensures Clackamas County can effectively respond to cyber threats, such as data breaches, ransomware attacks, or other cybersecurity incidents requiring coordinated action, as well as to infrastructure security threats to and incidents affecting County facilities. ESF-17 supports the Clackamas County Emergency Operations Center (EOC) by coordinating Security Operations (SecOps) and Incident Response (IR) with other resources to protect county systems, services, facilities, staff, and residents.

ESF 17 actions will facilitate, coordinate, and support the following core functions:

- **Share Information:** Facilitate timely cyber and physical security threat intelligence sharing among County departments, state, and federal agencies.
- **Monitor and Protect:** Maintain a cyber SecOps team to detect, monitor, and prevent cyber threats in real-time and a Facilities Management Security Team to identify infrastructure security threats and implement protective actions.
- **Respond and Recover:** Establish a cyber–Incident Response Team (IRT) to quickly detect, respond to, and recover from cybersecurity incidents and utilize the Facilities Management Security Team to respond to infrastructure security incidents.

1.2 Scope

ESF-17 provides a centralized framework to manage significant cyber and infrastructure security incidents impacting Clackamas County's infrastructure, services, staff, and residents. It ensures coordinated, consistent, and rapid response actions by:

- Clarifying roles and responsibilities for county departments and partner agencies.
- Outlining resources and processes for threat and incident detection, response, and recovery.
- Supporting coordination with local, state, and federal agencies to reduce the impact of cyber and infrastructure incidents.

The infrastructure security aspect of ESF 17 is focused on the protection of County facilities. While this directly affects the protection of building occupants, procedures for the protection of staff and visitors are provided in other County plans and programs including the County

Risk Management Manual and the AlertUs program and AlertAware app. The response to an individual or a group of people threatening to cause or actually causing damage to County facilities will be handled by the Sheriff's Office and local law enforcement in accordance with ESF 13: Law Enforcement.

1.3 Policies, Frameworks and Standards

Clackamas County Technology Services (CCTS) is responsible for enforcing technology policies and ensuring compliance with cybersecurity standards during ESF-17 activation, including:

- **Enforcement of Clackamas County Technology Policies:** The CCTS Security Team enforces the Acceptable Use of Technology Policy (EPP-59), ensuring county employees and systems adhere to guidelines for secure and appropriate technology use, reducing vulnerabilities during cyber incidents.
- **Compliance with Cybersecurity Standards:** CCTS aligns all ESF-17 activities with the following standards, as directed by the Chief Information Officer (CIO):
- Oregon Statewide Cyber and Information Security Standards: Ensures consistency with state-level requirements for cybersecurity practices and incident response.
- **Center for Internet Security (CIS) Controls Cybersecurity Framework:** Implements critical security controls to protect systems, detect threats, and respond effectively to incidents.
- **National Institute of Standards and Technology (NIST) SP 800-61 Revision 2:** Follows guidelines for incident response, including preparation, detection, analysis, containment, eradication, recovery, and post-incident activities.

Facilities Management is responsible for implementing the Facilities Management Team Security Levels Action Plan (FMP 3.02.019), which establishes Clackamas County security level standards for responding to infrastructure security threats and incidents.

2 Situation and Assumptions

2.1 Cybersecurity

Cybersecurity incidents such as data breaches, ransomware, or system disruptions can significantly affect Clackamas County's cyber infrastructure, services, staff, and residents. These incidents can happen independently or as a result of other emergencies, like natural disasters or infrastructure failures. An effective response and recovery effort requires coordinated actions to address cyber and physical impacts, ensuring resources are allocated to mitigate identified challenges.

The following assumptions guide planning and response for cybersecurity incidents under ESF-17, based on potential challenges and operational realities:

- **Multiple Cyber Incidents:** Simultaneous or cascading cyber incidents may overwhelm response capabilities. Strategic planning, training, and exercises are essential to prepare responders for managing multiple threats effectively.
- **Communication Challenges:** A major cyber or physical incident could disrupt communication systems critical for coordination. Secure, reliable, and flexible communication channels must be established to ensure public and private sector entities can collaborate when standard systems fail.
- **Expertise and Capacity Needs:** Responding to complex cyber incidents requires specialized technical expertise and the ability to scale resources during prolonged events. Clackamas County must plan for access to skilled personnel and surge capacity, potentially through partnerships with state and federal agencies.
- **Private Sector Coordination:** Private entities own or operate much of the county's critical infrastructure and cyberspace, limiting direct government control. Effective response depends on strong coordination with private sector partners to align efforts and share resources.

2.2 Infrastructure Security

Infrastructure security threats and incidents may arise from several sources including public protest activities or political or social unrest and from individuals conveying threats or acting with malicious intent. Infrastructure security threats may also arise from other emergencies such

as natural disasters which damage County facilities. The initial response to incidents damaging County facilities will be guided by this plan, but the longer-term restoration and recovery efforts will be managed in accordance with the County's Continuity of Operations (COOP) plans.

The following assumptions guide planning and response for infrastructure security threats and incidents under ESF-17, based on potential challenges and operational realities:

- **Multiple Threats/Incidents:** Simultaneous threats and/or incidents may overwhelm response capabilities. Strategic and tactical planning, training, and exercises are essential to prepare staff for managing multiple threats/incidents effectively.
- **Coordination Challenges:** Depending on the facility or facilities threatened or impacted, effective coordination with County leadership and other involved parties will be critical. This includes coordination with Risk Management and the Sheriff's Office and may include court security, contract security, and the Oregon City Police Department. Pre-planning with these departments and parties will help ensure an effective response.
- **Communication Challenges:** Communication with the occupants (staff and visitors) will be an important component of any infrastructure security response. Programs and tools such as AlertUs, AlertWare, and internal public address systems may be used to communicate information and instructions to building occupants. Providing emergency communications to building occupants is the responsibility of County leadership and Risk Management but will rely, in part, on effective coordination with Facilities Management regarding actions be taken to protect County infrastructure.

3 Concept of Operations

3.1 Cybersecurity Operations

3.1.1 General

Clackamas County Technology Services (CCTS) serves as the primary agency for managing cybersecurity incidents under ESF-17, coordinating federal, state, local, and public-private partnerships. Within the Concept of Operations, CCTS integrates cyber operations and incident response processes to ensure a unified response to cyber incidents. This includes leveraging Security Operations (SecOps) for continuous monitoring and threat detection, and the Incident Response Team (IRT) for rapid response and recovery, as outlined in NIST SP 800-61 Revision 2.

3.1.1.1 Preparation

- Develop and maintain cybersecurity policies, incident response plans, and playbooks.
- Train county staff and EOC personnel on cyber incident response procedures.
- Establish communication channels with state (e.g., Oregon TITAN Fusion Center) and federal agencies (e.g., CISA, FBI).

3.1.1.2 Detection and Analysis

- Monitor County networks and systems for suspicious activity using SecOps tools.
- Analyze potential incidents to determine scope, impact, and severity.
- Share threat intelligence with stakeholders to enhance situational awareness.

3.1.1.3 Containment, Eradication, and Recovery

- Contain incidents to limit damage, such as isolating affected systems.
- Eradicate threats by removing malicious code or restoring compromised systems.
- Recover by restoring normal operations and implementing lessons learned to prevent recurrence.
- Utilize off-site emergency solutions outlined in department COOP plan.

3.1.1.4 Coordination

- The EOC activates ESF-17 when a cyber incident disrupts County operations or services.
- The ESF-17 Coordinator, appointed by the CCTS Director, coordinates SecOps and IRT activities with the EOC.

- Coordinate with external partners, including state agencies, federal authorities, and private sector entities.

3.1.1.5 Responsibilities

- Clackamas County EOC: Activates ESF-17, provides resources, and ensures inter-agency coordination.
- CCTS SecOps Team: Monitors systems, detects threats, and implements preventive measures.
- CCTS Incident Response Team (IRT): Leads incident analysis, containment, eradication, and recovery efforts.
- County Departments: Report cyber incidents, support efforts, and follow ESF-17 guidance.
- External Partners: Provide threat intelligence, technical assistance, and regulatory guidance.

3.1.2 Cyber Incident Management Phases

Cybersecurity incidents require collaboration between information technology (IT) experts and emergency management teams. To ensure clear communication across these groups, the following matrix (Figure 17-1) illustrates how IT incident response activities align with emergency management phases. This framework uses terminology familiar to both stakeholders, promoting a unified approach to managing cyber incidents.

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

Emergency Management Phase	Cyber Incident Response Phase	Key Activities
Preparedness	Preparation	-Develop and update cybersecurity policies and incident response plans. -Conduct training and exercises for IT and emergency management teams. -Deploy security tools (e.g., firewalls, intrusion detection systems).
Preparedness	Preparation	-Establish communication channels with local, state, and federal partners. -Share threat intelligence to enhance situational awareness. -Test backup systems and response playbooks.
Response	Detection and Analysis	-Monitor systems to identify cyber threats or incidents. -Analyze incidents to determine scope, impact, and severity. -Notify stakeholders and activate the Incident Response Team (IRT).
Response	Containment	-Isolate affected systems to limit damage. -Implement short-term fixes to stop ongoing threats. -Coordinate with external partners (e.g., Oregon TITAN Fusion Center, FBI, CISA).

Emergency Management Phase	Cyber Incident Response Phase	Key Activities
Recovery	Eradication and Recovery	-Remove malicious code or restore compromised systems. -Verify systems are secure and restore normal operations. -Communicate updates to stakeholders and residents.
Recovery	Post-Incident Activity	-Document lessons learned and update response plans. -Conduct after-action reviews to improve future responses. -Share findings with partners to strengthen countywide resilience.

3.1.3 Cyber Incident Response Team

The Cyber Incident Response Team (IRT), facilitated by Clackamas County Technology Services (CCTS), is established to manage cybersecurity incidents impacting the County. The IRT operates within the ESF-17 framework, aligning with NIST SP 800-61 Revision 2 phases (Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity). Upon activation, the Chief Information Officer (CIO) within CCTS appoints IRT members. The IRT integrates cyber operations (monitoring and threat detection) and incident response (containment and recovery) to mitigate threats and restore services.

The IRT is responsible for executing and coordinating response efforts under ESF-17, including:

- **Tactical Response Operations:** Implement actions to detect, analyze, contain, eradicate, and recover from cyber incidents, aligning with the four lines of effort (Threat Response, Asset Response, Intelligence Support, and Affected Entity Response).
- **Strategic Alignment:** Follow guidance from the Clackamas County Emergency Operations Center (EOC) and governing authorities to ensure response actions support countywide objectives.
- **Coordination with Partners:** Collaborate with public and private sector entities, including the Oregon TITAN Fusion Center, FBI, CISA, and private cybersecurity vendors, to enhance threat detection, reporting, and response procedures.
- **Regular Reporting:** Establish a schedule to provide updates to the EOC, ensuring situational awareness and operational coordination. This includes:
    - Conducting briefings and sharing information with state, local, and private partners.
    - Submitting reports to federal entities (e.g., CISA, FBI) using designated procedures to meet regulatory requirements and maintain federal-level awareness.
- **Support for Investigations:** Assist law enforcement agencies with criminal investigations by facilitating evidence collection and ensuring proper handling to support legal processes.
- **Technical Assistance:** Provide technical support to affected entities (e.g., County departments or critical infrastructure operators) to resolve incidents, mitigate vulnerabilities, and restore systems.
- **Information Sharing:** Coordinate with the EOC to disseminate threat intelligence and

incident updates, fostering collaboration across stakeholders to reduce the impact of cyber incidents.

3.1.4 Cyber Incident Response Lines of Effort

To effectively manage cyber incidents, ESF-17 organizes response activities into four concurrent lines of effort: Threat Response, Asset Response, Intelligence Support, and Affected Entity Response. These lines of effort, detailed in Table 17-1, provide a framework to synchronize actions before, during, and after a cyber incident, ensuring a coordinated and efficient response.

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

Line of Effort	Definition
Threat Response	-Activities led by law enforcement and cybersecurity teams to address the threat: -Collect evidence and intelligence to identify the source of the incident. -Link related incidents and identify other potential targets. -Pursue and disrupt threat activities. -Develop and execute actions to neutralize immediate threats.
Asset Response	-Technical assistance to protect systems and reduce incident impacts: -Identify at-risk entities and assess vulnerabilities. -Evaluate risks to the county or region, including cascading effects. -Develop actions to mitigate risks and support recovery. -Coordinate with threat response teams to share information. -Guide the use of local and state resources for rapid recovery.
Intelligence Support	-Build situational awareness and share intelligence to support response: -Analyze threat trends and events to inform response efforts. -Identify and address knowledge gaps. -Recommend ways to counter or reduce adversary capabilities. -Share intelligence with county, state, and federal partners (e.g., Oregon TITAN Fusion Center, FBI, CISA).
Affected Entity Response	-Encourage entities impacted by the incident to participate actively: -Share incident details with cybersecurity teams to aid investigation, response, and recovery. -As data owners, take responsibility for implementing safeguards and remediation measures to secure systems and prevent future incidents.

3.2 Infrastructure Security Operations

3.2.1 General

Clackamas County Facilities Management serves as the primary coordinating agency for access and infrastructure security for County facilities under ESF-17 in partnership with County leadership, Risk Management, the Sheriff's Office, the Oregon City Police Department (OCPD), and others as appropriate for the situation and location. This responsibility is shared with the Sheriff's Office and OCPD when an individual or groups of people are threatening to cause or

actually causing damage to County facilities. Within the Concept of Operations (ConOps), the Facilities Management response will be guided by the Security Levels Action Plan and direction from County leadership.

3.2.2 Existing Systems and Capabilities

Facilities Management utilizes numerous methods and means to protect County buildings on a day-to-day basis. The methods and means range from the use of access control systems and cameras to the installation of fencing, bollards/barricades, window film, and ballistic glass. These methods and means are guided by historical information and utilization of new technology.

3.2.3 Threat/Incident Detection and Alerting

Threats to county facilities may be detected or identified in many ways. They may be conveyed in writing (letter, email, social media post) or orally (phone, in person), identified through routine law enforcement investigative work, or recognized as a threat based on past incidents. Actual incidents (past or in progress) will most likely be detected by staff in the course of normal work or through community member reporting.

Regardless of the means of detection, County leadership, Risk Management, Facilities Management, and the Sheriff's Office need to be alerted so appropriate infrastructure protection actions can be determined and implemented.

3.2.4 Threat Levels

The Facilities Management Security Levels Action Plan provides the framework to guide County leadership and Facilities Management staff actions in response to infrastructure security threats. The plan identifies levels of threat ranging from normal, day-to-day concerns to actual incidents with extreme security impacts, and identifies actions to be considered or taken for each level of threat including activation of the Facilities Management Security Team, Security Emergency Command Center (SECC), and County Emergency Operations Center (EOC) and communication with County staff and the public, where necessary.

Based on the threat level, County leadership and Facilities Management will collaboratively determine what, if any, additional security measures will be implemented. This may include:

- Limiting building access
- Installing additional cameras, fencing, lighting, and/or barricades
- Real-time monitoring of security and building systems
- On-site reporting
- Arranging for contract security services or additional law enforcement patrols

3.2.5 Facilities Management Security Team

The Facilities Management Security Team includes Facilities Management staff pre-identified to respond to infrastructure security threats and staff the Security Emergency Command Center.

The team will normally be activated consistent with the Security Levels Action Plan but may be activated at any threat level to coordinate and implement infrastructure security actions.

3.2.6 Facilities Management Security Emergency Command Center (SECC)

The Facilities Management Security Emergency Command Center (SECC) is the location from which the Facilities Management Security Team operates during heightened threat levels to direct and coordinate its infrastructure security operations. The SECC is located adjacent to the County EOC and will coordinate its actions with the EOC when it's activated.

3.3 Coordination with Other ESFs

The following ESFs support ESF 17-related activities:

- **ESF 2, Communications:** Augment communications resources to county, local, state, and federal agencies.
- **ESF 3, Public Works:** Assist with the placement of infrastructure security systems (e.g., barricades).
- **ESF 13, Law Enforcement:** Provide support for law enforcement resources, investigations, and reports.
- **ESF 15, Public Information:** Develop staff and public messaging in support of infrastructure security actions.

4 Emergency Coordination

4.1 Cybersecurity

Clackamas County Technology Services (CCTS), led by the Chief Information Officer (CIO), serves as the primary agency for coordinating cybersecurity incident response under ESF-17. Within the Concept of Operations (ConOps), the CIO facilitates information and resource sharing among diverse stakeholders, ensuring a unified response to cyber incidents. This coordination aligns with NIST SP 800-61 Revision 2 phases (Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity) and adheres to all applicable county policies, Oregon Statewide Cyber & Information Security Standards, and CIS Controls Cybersecurity Framework. The CIO integrates cyber operations (monitoring and threat detection) and incident response (containment and recovery) to support effective collaboration across partners.

4.1.1 Responsibilities

- **Intergovernmental Coordination:** Facilitate collaboration with federal agencies (e.g., CISA, FBI), state entities (e.g., Oregon TITAN Fusion Center), local governments, tribal partners, and emergency management to share threat intelligence, align response actions, and access resources.
- **Public-Private Partnerships:** Act as a conduit for intelligence, equipment, expertise, and staff between public sector partners (e.g., law enforcement, emergency management) and private sector entities (e.g., critical infrastructure operators, cybersecurity vendors).
- **Information and Resource Sharing:** Centralize the dissemination of cyber threat intelligence and incident updates to ESF-17 partners, ensuring timely and accurate communication to support operational coordination.
- **Support for Incident Response:** Work with the Incident Response Team (IRT) to provide technical assistance, facilitate evidence collection, and ensure compliance with CIO-directed standards during incident response and recovery.

4.2 Infrastructure Security

Clackamas County Facilities Management serves as the primary agency for coordinating infrastructure security incident response under ESF-17. The Facilities Management Security Team facilitates the sharing of threat level information and coordinates the implementation of

enhanced infrastructure security measures with internal and external partners. These actions are guided by the Facilities Management Security Team Security Levels Action Plan (FMP 3.02.019).

4.2.1 Responsibilities

- **Internal and External Agency Coordination:** Facilitate coordination with County leadership, the Sheriff's Office, the County EOC (when activated), and when appropriate, the Oregon City Police Department for Oregon City-based County facilities, and other local law enforcement agencies for remote facilities. This collaboration will focus on the sharing of threat information, infrastructure security measure decision-making, and alignment of response actions.
- **Staff and Public Messaging:** Work with County leadership and Public & Government Affairs (PGA) to develop and disseminate staff and, where appropriate, public messaging related to the infrastructure security threat and security measures in place.
- **Support for Incident Response:** Provide assistance to County staff with the implementation of infrastructure security measures and work with the County EOC (when activated) to secure additional resources needed to support the response.

5 ESF Annex Development and Maintenance

5.1 Cybersecurity

Clackamas County Technology Services (CCTS) oversees the ongoing review and maintenance of the cybersecurity components of the ESF-17 annex, ensuring it remains current and effective in addressing cybersecurity incidents. Within the Concept of Operations (ConOps), CCTS aligns this process with NIST SP 800-61 Revision 2 guidelines, particularly the Post-Incident Activity phase, to incorporate lessons learned and update plans. CCTS collaborates with primary and supporting agencies to maintain compliance with the Acceptable Use of Technology Policy (EPP-59), Oregon Statewide Cyber & Information Security Standards, and CIS Controls Cybersecurity Framework, supporting a robust cybersecurity posture.

5.1.1 Responsibilities

- **Intergovernmental Coordination:** Facilitate collaboration with federal agencies (e.g., CISA, FBI), state entities (e.g., Oregon TITAN Fusion Center), local governments, tribal partners, and emergency management to share threat intelligence, align response actions, and access resources.
- **Public-Private Partnerships:** Act as a conduit for intelligence, equipment, expertise, and staff between public sector partners (e.g., law enforcement, emergency management) and private sector entities (e.g., critical infrastructure operators, cybersecurity vendors).
- **CCTS Coordination:** CCTS is responsible for coordinating regular reviews and updates of the ESF-17 annex, ensuring alignment with evolving cyber threats, County policies, and industry standards. This includes scheduling annual reviews, incorporating feedback from exercises and incidents, and disseminating updates to stakeholders.
- **Agency Responsibilities:** Each primary and supporting agency (e.g., Emergency Operations Center, Incident Response Team, and external partners) must develop and maintain plans and procedures to address their assigned tasks under ESF-17. Agencies are expected to:
    - Update internal response playbooks to reflect ESF-17 requirements.

- Participate in review processes and provide input to CCTS.
- Ensure compliance with CIO-directed standards during plan development.

5.2 Infrastructure Security

Clackamas County Facilities Management oversees the ongoing review and maintenance of the infrastructure security components of the ESF-17 annex, ensuring it remains current and effective in addressing infrastructure security incidents.

5.2.1 Responsibilities

- **Facilities Management Coordination:** Facilities Management will provide subject matter expertise during coordinated regular reviews and updates of the ESF-17 annex, ensuring alignment with evolving infrastructure security threats and County policies. This includes scheduling annual reviews, incorporating feedback from exercises and incidents, and disseminating updates to stakeholders.
- **Agency Responsibilities:** Each primary and supporting agency (e.g., CCSO, Risk Management, Public & Government Affairs, Disaster Management) must develop and maintain plans and procedures to address their assigned tasks under ESF-17. Agencies are expected to:
  - Update internal response playbooks to reflect ESF-17 requirements.
  - Participate in review processes and provide input to Facilities Management.
  - Ensure compliance with County policies during plan updates.