Cybersecurity & Infrastructure Security Agency

Prepared for the State of Oregon

CISA/ICTAP-OR-AFTACTRPT-004-R0

Oregon Cybersecurity TTX/FE AAR/IP
March 2022

State of Oregon – Gremlins in the Gears Cybersecurity Tabletop Exercise and Functional Exercise

After Action Report and Improvement Plan

This document was prepared for the State of Oregon by the DHS Cybersecurity and Infrastructure Security Agency (CISA), Interoperable Communications Technical Assistance Program (ICTAP) as part of Work Order # WO22-012. Additional information about the program can be found at https://www.cisa.gov/safecom/ictapscip-resources.

This page intentionally left blank

EXECUTIVE SUMMARY

The State of Oregon Statewide Interoperability Coordinator (SWIC) requested assistance from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency Interoperable Communications Technical Assistance Program (CISA/ICTAP) to conduct a tabletop exercise (TTX) and brief Functional Exercise (FE) addressing current cybersecurity plans and procedures in Public Safety Answering Points (PSAP) in the Lane County area. After completion of the TTX and FE, this After-Action Report/Improvement Plan (AAR/IP) was created to identify gaps and make recommendations for improving cybersecurity in communications across the State of Oregon.

Overview

The Oregon Gremlins in the Gears Cybersecurity TTX took place on the morning of January 6, 2022, immediately followed by the Oregon Gremlin in the Gears Cybersecurity FE, that afternoon. Both the TTX and FE were conducted in-person at the Springfield Justice Center in Springfield, Oregon. The TTX included a webinar format for attendees that were unable to meet in-person. 41 participants from 20 agencies attended the TTX, and of those, 30 participants from 15 agencies attended the FE.

The suggested actions in this report should be viewed as recommendations only. In some cases, agencies may determine the benefits of implementation are insufficient to outweigh the costs. In other cases, agencies may identify alternative solutions that are more effective or efficient. Each agency should review the recommendations and determine the most appropriate action and the resources needed (i.e., time, staff, and funding) for implementation.

Key Findings

The Oregon Gremlins in the Gears Cybersecurity TTX/FE AAR/IP identifies critical considerations and associated recommendations regarding cybersecurity in interoperable communications across the state. This report can be used to help the state improve overall cybersecurity in interoperable communication, and regional agencies can develop priorities and focus their efforts on achieving and improving emergency communications cybersecurity.

This TTX/FE highlighted several successes associated with overall cybersecurity:

- Participation of key personnel and agencies to identify the shortfalls of the region when cybersecurity for the radio system is concerned.
- Collaboration among the tri-county region for operational communications collaboration was effective and the group shared a good sense of the procedures and necessary steps to keep communications operational.
- State of Oregon Cyber Security Services (CSS) in cooperation with CISA Cybersecurity representatives shared timely and important information with the participants of the exercise.
- State of Oregon CSS provides important cybersecurity resources to responding agencies across the state.
- Nontraditional communications personnel were put into different positions outside their comfort zone and were able to make operational decisions and create communication talkpaths that worked.
- Presentations from agencies that have been impacted by recent cybersecurity incidents provided insight into the potential risk that agencies face.

- Coordination between ESF2 and the newly developed ESF17 (Cybersecurity) positions is excellent.

The Oregon Gremlins in the Gears Cybersecurity TTX/FE also identified several opportunities for improving cybersecurity in communications. These gaps, detailed in Section 4 of the AAR/IP, offer insight into findings documented during the planning and execution phases of the TTX/FE.

Major recommendations include:

- Document escalation procedures to provide guidance for declaring a cyber incident and activating incident response to include notification of interconnected system authorities.
- Develop or update existing Continuity of Operations Plan (COOP) and Disaster Recovery (DR) plans to include response to cybersecurity incidents.
- Develop or update existing Cyber Standard Operating Procedures (CSOP) for configuring and operating information system account privileges.
- Apply CSOPs to systems from the very beginning, even during buildup and testing phases.
- Review current Service Level Agreements (SLAs) with infrastructure vendors to ensure those agreements address cybersecurity requirements.

Conclusion

The Oregon Gremlins in the Gears Cybersecurity TTX/FE is an essential step toward increasing and improving cybersecurity in communications in the State of Oregon. By continually assessing progress and making improvements, public safety entities across the state will continue to excel in their dedication to disaster preparedness and their mission to achieve an optimal level of secure interoperable communications throughout the state. Their efforts to date have been exemplary and will serve the area admirably for years to come.

TABLE OF CONTENTS

1 INTRODUCTION

The mission of the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency Interoperable Communications Technical Assistance Program (CISA/ICTAP) is to unify and lead the nationwide effort to improve cybersecurity and emergency communications capabilities across all levels of government. More information about CISA and other CISA work products related to interoperable communications can be found at https://www.cisa.gov/safecom.

The State of Oregon Statewide Interoperability Coordinator (SWIC) requested assistance from CISA/ICTAP to conduct a tabletop exercise (TTX) and brief Functional Exercise (FE) addressing current cybersecurity plans and procedures in Public Safety Answering Points (PSAPs) in the Lane County area. After completion of the TTX and FE, this After-Action Report/Improvement Plan (AAR/IP) was created to identify gaps and make recommendations for improving cybersecurity in communications across the State of Oregon.

1.1 Exercise Overview

The Oregon Gremlins in the Gears Cybersecurity TTX took place on the morning of January 6, 2022, immediately followed by the Oregon Gremlins in the Gears Cybersecurity FE that afternoon. Both the FE and TTX were conducted in-person at the Springfield Justice Center in Springfield, Oregon. The TTX included a webinar format for attendees that were unable to meet in-person. 41 participants from 20 agencies attended the TTX, and of those 30 participants from 15 agencies attended the FE.

The suggested actions in this report should be viewed as recommendations only. In some cases, agencies may determine the benefits of implementation are insufficient to outweigh the costs. In other cases, agencies may identify alternative solutions that are more effective or efficient. Each agency should review the recommendations and determine the most appropriate action and the resources needed (i.e., time, staff, and funding) for implementation.

CISA/ICTAP uses a first responder-driven approach to obtain unvarnished input from participants. This approach minimizes ambiguity and helps ensure effective cybersecurity and interoperable communications solutions are identified and implemented.

Event Type

Tabletop Exercise and Functional Exercise

Exercise Name

Oregon Gremlins in the Gears Cybersecurity Tabletop Exercise/Functional Exercise

Exercise Date

January 6, 2022

Duration

8 hours

Location

Springfield Justice Center in Springfield, Oregon

Sponsor

State of Oregon

Scenario Type

Cyber Attack

1.2 Exercise Planning Team

The Gremlins in the Gears generated an increased awareness of existing cybersecurity solutions and also highlighted the need for future cooperation and coordination across jurisdictions and agencies. Through their own continued efforts and by building on the results of the TTX and FE, local agencies and jurisdictions throughout Oregon are encouraged to continue to improve cybersecurity in their PSAPs and communications systems. Included in Appendix B is a list of Exercise Planning Team (EPT) members.

1.3 Participants

1.3.1 Participant Roles

- **Players** – First responders and communication specialists who responded to the situation presented based on their current knowledge of response procedures, plans, cross-jurisdictional agreements, and communication capabilities.
- **Observers** – Agency and subject matter expert personnel who did not play during the exercise but who watched the session and provided their inputs via the Hotwash.
- **Evaluators** – CISA/ICTAP subject matter experts who documented the exercise and interpreted exercise outcomes for inclusion in the AAR/IP.
- **Facilitators** – Individuals controlling/conducting the TTX who provided situation updates and moderated the conversations.
- **Controllers** – Individuals controlling/conducting the FE who provided situation updates and exercise injects to which players were expected to respond.

Players	16
Observers	19
Controller/Evaluators	4
Facilitator	2
Total Participants	41

1.3.2 Participating Agencies & Organizations

Exercise participants (listed in Appendix C) included representatives from the following organizations.

Local Agencies (13 total)

- Central Lane 9-1-1
- City of Eugene Information Technology
- City of Eugene Public Works
- City of Eugene Radio Shop
- City of Springfield

- Eugene Police Department
- Lane County
- Lane County Information Technology
- Lane County Technology Services
- Lane County Sherriff's Office
- Linn County Sherriff's Office
- Multnomah County
- Washington County Emergency Management

State Agencies (5 total)

- Oregon Enterprise Information Services Cyber Security Services
- Oregon Department of Human Services Emergency Management Unit
- Oregon Department of Justice – Fusion Center
- Oregon Enterprise Information Services – Shared Services - Statewide Interoperability
- State of Oregon SWIC's Office

Federal Agencies (1 total)

- DHS/CISA

Other Agencies (1 total)

- Adcomm Engineering

2 DESIGN

2.1 Purpose

The Gremlins in the Gears TTX/FE provided an opportunity to evaluate current cybersecurity concepts, plans, and capabilities as they pertain to cybersecurity in communications across jurisdictions within Oregon.

2.2 Scope

Gremlins in the Gears focused on discussing and demonstrating key cybersecurity risks, plans, and procedures within and across participating agencies.

Outcomes from Gremlins in the Gears included a better understanding of the risks, successes, and gaps associated with cybersecurity within PSAPs and communications systems. Evaluation measures included policies, plans, and capabilities. Consistent with Homeland Security Exercise and Evaluation Program (HSEEP) guidelines, an improvement plan is appended to this AAR (see Appendix A).

Gremlins in the Gears was not designed to focus on personnel competency; rather, it was designed to focus on concepts, policies, plans, and procedures for response to a cybersecurity attack, breach, or threat.

2.3 Capabilities

The National Planning Scenarios[1] and the establishment of the National Preparedness Guidelines[2] steered the focus of homeland security toward a capabilities-based planning approach. Capabilities-based planning focuses on planning under uncertainty, as the next danger or disaster can never be forecast with complete accuracy. Therefore, capabilities-based planning takes an all-hazards approach to planning and preparation, which builds capabilities that can be applied to a wide variety of incidents.

For the past several years, states and urban areas have used capabilities-based planning to perform baseline assessments of their homeland security efforts by comparing their current capabilities against the Target Capabilities List (TCL)[3] and the Emergency Support Function (ESF)[4] annexes. This approach identified gaps in current capabilities and focused efforts on identifying and developing priority capabilities and tasks for the jurisdiction.

In September 2011, DHS released the first edition of the National Preparedness Goal[5] in response to Presidential Policy Directive 8: National Preparedness (PPD-8). The National Preparedness Goal describes our nation's security and resilience posture through Core Capabilities, which represent an evolution from the TCL. The Core Capabilities address five mission areas (Prevention, Protection, Mitigation, Response, and Recovery). Each Core Capability includes preliminary capability targets.

---

[1] National Planning Scenarios: https://www.fema.gov/txt/media/factsheets/2009/npd_natl_plan_scenario.txt
[2] National Preparedness Guidelines: http://www.fema.gov/pdf/emergency/nrf/National_Preparedness_Guidelines.pdf
[3] Target Capabilities List: http://www.fema.gov/pdf/government/training/tcl.pdf
[4] ESF Annexes: http://www.fema.gov/pdf/emergency/nrf/nrf-esf-all.pdf
[5] National Preparedness Goal: http://www.fema.gov/pdf/prepared/npg.pdf

The EPT selected the capabilities listed below for this event. These capabilities provided the foundation for the development of the event schedule and participating entities. The EPT selected the following Core Capabilities:

- Operational Communications
- Operation Coordination
- Cybersecurity

2.4 Goal and Objectives

The goal of the Gremlins in the Gears was to discuss cybersecurity and communications policies, procedures, plans, available assets, and capabilities used by regional agencies in response to a significant multi-jurisdictional incident or event, especially where the necessary overlap is between the two disciplines.

These exercises focused on the following objectives:

- Engage stakeholders of the regional interoperable communication system(s), to discuss the operations and applications of the system(s) in the occurrence of a cybersecurity compromise.
- Identify redundant interoperable communication capabilities in the event of major disruptions to the primary communication system(s) during a cybersecurity related incident.
- Discuss the ability of the participating public safety personnel to rapidly and effectively establish interoperable communications in the case of a major, multi-agency cybersecurity incident.
- Review the operable and interoperable communications available to or required by exercise participants in accordance with existing operational procedures and regional response cybersecurity plans.
- Identify and discuss the necessary notification pathways that are necessary during a cybersecurity related incident.
- Engage private partners to work with public safety entities to solve cybersecurity related problems.
- Enhance the overall readiness of the region in the event of an actual emergency involving a large-scale cybersecurity incident.

2.5 Hotwash

After completing each exercise segment (the TTX and the FE), Players, Observers, and support personnel received opportunities to discuss the exercises with each other during a facilitated Hotwash session. The Hotwash provided all participants a chance to share their observations, correct misconceptions, and help improve cybersecurity in communications. Both exercise play and Hotwash notes/comments were consolidated through a process that identifies and discusses event findings and methodologies to address challenges faced by participating agencies.

3 SCENARIOS

The exercise scenarios were developed locally in collaboration with the EPT. They are unique to the State of Oregon. Exercise planners incorporated critical communication cybersecurity elements into Gremlins in the Gears. The cybersecurity focus provided an opportunity to identify and document gaps in current capabilities and processes. The cybersecurity focus also sparked productive discussions among scenario players that enabled the sharing of different approaches and operating procedures with other jurisdictions.

The scenarios used for Gremlin in the Gears are below:

TTX Scenario 1 – Dispatch Connectivity

It is a fairly normal day in the county. There are a few activities going on that responders are watching closely, like a protest at the campus, but that is just another Tuesday. Around 9am a call comes into Central Lane County Dispatch from a patrol officer asking why they are not answering on the radio. Upon further investigation, the supervisor on duty realizes that they are not able to transmit or receive on the radio system.

TTX Scenario 2 – Radio System Cyber Policies

Responders from around the region are calling into dispatch via cell phone to report that they are not able to transmit outside of their local area. They cannot reach dispatch, their supervisors, or anyone else that is not in visual range. They are also unable to change it to another channel and the radio switched away from their dispatch channel. Dispatch has no indication of a problem on their consoles.

TTX Scenario 3 – Radio System Compromise and Mitigation

During a planned upgrade to a new operating system version, all of the field responders start to receive FAILSOFT on their displays. Dispatch has called to the system administrator and informed him that there are several responders in the southwest portion of Eugene that are all experiencing FAILSOFT on their radios and unable to transmit outside car to car channels. Other systems not connected to the radio system are also compromised. The city email and internet is also down.

FE Scenario 1

You have identified that a server about to go online in the radio system has been infected with malware.

FE Scenario 2

Central Lane County Dispatch has lost connectivity with the Regional Radio System. They still have working phone lines and are able to receive 9-1-1 calls for service. Central Lane County Dispatch is requesting your Communications Unit take over some of the calls for service dispatching for them. They will provide you with a list of six Police units you will be responsible for. Central Lane County Dispatch will only give you the calls they want you to dispatch. While Central Lane County Dispatch is down, your dispatching will be conducted on test talkgroup.

The standard asset ordering process must be used to request any equipment your Communications Unit will need to accomplish this. Your assigned location is the Springfield Justice Center parking lot.

FE Scenario 3

The Quarry Hill radio tower site has gone into Site Trunking mode.

4 GAP ANALYSIS

The Gremlins in the Gears AAR/IP baselines communications cybersecurity, identifies gaps, provides recommendations, and can be used to help the state improve communications cybersecurity. With this knowledge, agencies can develop priorities and focus their efforts on achieving and improving communications cybersecurity.

Gremlins in the Gears highlighted several communications cybersecurity successes associated with public safety in Oregon:

- Participation of key personnel and agencies to identify the shortfalls of the region when cybersecurity for the radio system is concerned.
- Collaboration among the tri-county region for operational communications collaboration was effective and the group shared a good sense of the procedures and necessary steps to keep communications operational.
- State of Oregon Cyber Security Services (CSS) in cooperation with CISA Cybersecurity representatives shared timely and important information with the participants of the exercise.
- State of Oregon CSS provides important cybersecurity resources to responding agencies across the state.
- Nontraditional communications personnel were put into different positions outside their comfort zone and were able to make operational decisions and create communication talkpaths that worked.
- Presentations from agencies that have been impacted by recent cybersecurity incidents provided insight into the potential risk that agencies face.
- Coordination between ESF2 and the newly developed ESF17 (Cybersecurity) positions is excellent.

The exercises also identified several opportunities for improving communications cybersecurity. Participant responses revealed gaps in regional communications cybersecurity capabilities that should be viewed simply as deficiencies in cybersecurity methods, processes, and/or systems.

Exercise activities identified several opportunities for improving cybersecurity communications proficiency when responding to a cybersecurity incidents. The challenges and related recommendations are detailed below.

4.1 Identification and Declaration of Cybersecurity Incident

Description: It was clear there was no defined procedure or mechanism to “trigger” a cyber response. The Radio Technicians were focused in their silo and there did not appear to be anyone in the ecosystem that would likely identify a cyber incident as such. The participants immediately went into troubleshooting mode with no evidence of escalation[6] or notification of any other departments, entities or organizations. A notification roster for emergency situations was mentioned, but it does not cover technical/cyber issues. Focusing on the radio infrastructure while ignoring the potential of a cybersecurity incident would delay identification of the root cause of the problem. Consideration of trigger points would allow the team to recognize the difference between a standard Radio Access Network (RAN) problem and a cybersecurity incident. The participants did not discuss contacting a local Information Technology (IT) department to help with the issue.

[6] In cybersecurity terms “escalation” means elevating the level of troubleshooting or expertise.

Recommendations:

1. Train personnel to notify a supervisor or higher authority in any instance where software or hardware is not operating as intended.
2. Train supervisors to assess and determine the type of incident (e.g., hardware failure, software flaw, cyber incident).
3. Document escalation procedures to provide guidance for declaring a cyber incident and activating incident response to include notification of interconnected system authorities.

4.2 COOP and Disaster Recovery Plans

Description: Participants had some discussion of Continuity of Operations (COOP) Plans; however, there was consensus that no COOP plan existed for the relevant systems. The PSAPs themselves likely have COOP plans and cyber should be incorporated into them, if it isn't already.

Participants believed they may have documented Disaster Recovery (DR) plans. DR plans are used when business operations are impacted by a disaster and IT infrastructure is non-recoverable. The focus of DR plans is on rebuilding or recovering an environment from a disaster.

The COOP and DR plans are important, and personnel need to know where the plans are and which plan to execute. Training and exercise regimens should be updated to incorporate COOP and DR plans. Specialized training for one or more individuals would result in the identification of an Incident Manager who would correctly determine which plans requires activation.

Oregon has state level legislation requiring 9-1-1 Centers to have DR plans and what those plans must include.

403.150[7] Disaster recovery plan: A 9-1-1 jurisdiction must have a disaster recovery plan for the components of the emergency communications system within the 9-1-1 service area. The disaster recovery plan must include at a minimum:

1. Recovery procedures for service that is interrupted, preventing transmission of an emergency call to the primary public safety answering point and corresponding secondary public safety answering points. This may include, but is not limited to, a hard-wired alternative route or a plan on file with the provider designating alternative routes or answering points.
2. A plan to switch public safety answering point operations to an alternate site in the event the primary public safety answering point becomes inoperable.
3. 24-hour emergency numbers for the providers serving the 9-1-1 jurisdiction. In addition to these state requirements, agency DR plans should also include how a 9-1-1 call is routed from first ring to call completion during a cyber incident.

Recommendations:

1. Update existing COOP to include response to cybersecurity incidents.
2. Update existing DR plans to comply with §403.150 and include response to cybersecurity incidents.
3. Incorporate 9-1-1 call handling procedures during cyber incidents into DR plans.
4. Incorporate COOP and DR plans into future training and exercises.

[7] Formerly 401.775; 2015 c.247 §15

4.3 Cybersecurity Awareness Training

Description: Basic cybersecurity awareness training was not mentioned by participants during the exercise. The proper procedure for identifying, reporting, declaring, and escalation a cyber incident is not intuitive and need to be trained. This training should include secure operation of systems, access and password management, safe application use, incident response, reporting procedures, and authenticator (password) safety. Basic training is just that, basic. There are personnel who, by the nature of their position or responsibilities, require advanced cybersecurity training. System administrators, shift supervisors, IT and radio technicians responsible for maintenance of the system to name a few, should be trained in the detection and response to a cybersecurity incident.

CISA has developed a downloadable Cybersecurity Workforce Training Guide. The Guide helps staff develop a training plan based on their current skill level and desired career path. CISA offers over 100 training courses and certification prep materials as well as cybersecurity resources from across the federal government to help professionals stay current and advance their careers. This guide can be found on the Cybersecurity Workforce Training Guide website: https://www.cisa.gov/publication/cybersecurity-workforce-training-guide.

Recommendations:

1. Develop cybersecurity awareness training for users, technicians, and supervisors with specialized training for those in administrative or supervisory positions.
2. Provide cybersecurity awareness training for all users of all systems.
3. Provide advance cybersecurity training for those personnel whose position or duties dictate.

4.4 IT Account Control

Description: Agencies have partially implemented the use of separate accounts with elevated privileges for technicians. These accounts are separate from those with standard privileges. Completing this implementation should be prioritized and the elevated privilege accounts need to require multi-factor authentication (MFA). Dispatchers stated they routinely leave consoles logged in. Operational needs drive this behavior; however, implementation of compensating controls would facilitate audit and accountability records required for investigative purposes.

Cyber controls should be implemented first when building up a new system, not relaxed. It ensures personnel are comfortable operating in the secured environment and that the controls do not break the functionality. It is common to relax the controls for expediency and later seek process control exceptions when it is determined the hardening process impacts functionality. This leaves the environment vulnerable.

Recommendations:

1. Develop or update existing Cyber Standard Operating Procedures (CSOP) for configuring and operating information system account privileges.
2. Train personnel on CSOPs as part of the cyber awareness training.
3. Apply CSOPs to systems from the very beginning, even during buildup and testing phases.

4.5 Dependence on Vendors for Security

Description: The Tri-County Region has a contract with Motorola to provide monitoring of the health and security of the Regional Radio System. It was not clear whether the organization has conducted a risk analysis for this arrangement, nor have they investigated the controls

Motorola has in place. Vendor security assistance should be clearly documented and outlined in a Service Level Agreement (SLA), which should contain contact information, hours of availability, rules for contact and reporting, as well as expected response time. The service agreement between the vendor and the Tri-County Region should require the vendor to submit proof of passing a security audit such as ISO27001 or similar on a regular basis. This agreement should also compel the disclosure of known defects in the platform, potential "zero-day"[8] vulnerabilities, and change activities initiated, etc.

Oregon CSS has many resources for managing cyber with vendors, including contract language, standards for compliance, and system security plan templates. The CSS Oregon Cyber Disruption Response & Recovery - Voluntary Resource Guide for Local Government Quick Sheet can be found in Appendix E.

Recommendations:

1. Review current SLAs with infrastructure vendors to ensure those agreements address the cybersecurity requirements described above.
2. Consider the cybersecurity requirements described above in future SLA negotiations.

4.6 System Notifications and Coordination

Description: A variety of potential notification paths were identified based on a consensus of the group. These notifications and their triggers should be incorporated into a process that is followed during service interruptions. This process should include a Primary, Alternate, Contingent, Emergency (PACE) plan where redundant notification paths are selected to ensure that the message is deliverable in the event one or more of the paths are unavailable. Documented call trees or notification lists serve as guidance on who to call and when it is necessary to do so. Problem escalation notification procedures are included in Incident Response, COOP, or DR plans.

Participants were unaware whether there are any conflicting cyber policies among all the entities connected to their network, especially those that might put other connected environments at greater risk than they realize.

Recommendations:

1. Document when escalation procedures are implemented, declaring a cyber incident and activating incident response to include notification of interconnected system authorities.
2. Develop separate communication plans to inform/involve the technical staff from all the IT groups supporting the system and the radio technicians.
3. Continue using the Oregon Emergency Response System (OERS) mechanism for resource requests but also add another level of notifications to cyber or communications representatives to allow for quicker response.
4. Coordinate with any network connected entities to align cyber policies.

4.7 Command and Control of Tech Related Incidents

Description: A single person should be identified to coordinate all response activities during an outage. In the IT world, this would be governed under the Major Incident Process and managed by a person acting in the role of an Incident Manager. This person will help ensure the troubleshooting efforts do not conflict or further destabilize the system. This person helps maintain a broad view of the situation and is focused on identifying systemic issues including

[8] A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched.

those resulting from a cyber-attack. The Incident Manager role would own the decision rights outright (or be the representative or the person who does) for whether a "disaster" will be declared triggering the execution of the COOP and/or DR plans. An important aspect of incorporating IT into communications is to develop a common vernacular (e.g., "isolated network" to an IT network person likely means dedicated virtual local area network (VLAN) and subnet; to the radio people, they are likely expecting a separate physical network infrastructure).

Recommendations:

1. Cross train radio technician personnel in the IT Major Incident Process and the Incident Manager position.
2. Consider using a Unified Command type response, consisting of communications and IT personnel when the Regional Radio System suffers a cyber incident.
3. Create a commonality of terms quick reference card listing the terms used by IT and Communications Technicians.

4.8 Personnel Redundancy

Description: The Regional Radio System is supported by a dedicated group of knowledgeable individuals the user agencies can turn to when problems arise. However, this group can be narrowed down to one or two individuals that everyone turns to. This is because these singular individuals are the most knowledgeable and have the most historic and institutional knowledge of the radio system and all its parts and pieces. The theory is that these individuals never take vacation, are never impacted by the incident, and are always just a phone call away. The reality is none of that is true, as is evidenced by the fact that neither of the two go-to people were available during the exercise. A vast majority of the knowledge they possess did not come from reading a book or attending a training session. It comes from real world working experience maintaining the equipment and building relationships over years of just doing the job. Most system owners rarely think of what they will do when these people are not available or retire.

It is important that system owners plan for the temporary or permanent loss of their trusted and knowledgeable personnel. Implementing a mentoring program to impart as much information from one generation of system support personnel to the next can help alleviate the disastrous effects a retirement can cause.

CISA/Safecom has a publication that provides planning resources for public safety communications personnel. This publication can be accessed at: https://www.cisa.gov/sites/default/files/publications/Succession_Planning_Guide_FINAL_07-28-2020-508c.pdf.

Recommendations:

1. Consider implementing a mentoring program for key system support personnel.
2. Consider implementing a shadowing program for potential successors of key personnel.
3. Consider developing formal documentation for contacts and procedures to address radio system problems so that the system is not reliant on informal institutional knowledge of a limited number of people.

4.9 Formalized Talkpath Functionality Documentation

Description: Players associated with Dispatch Centers stated the Centers have an internal process to identify what talkpaths will work in certain areas. The process has not been formalized nor has this information been generally shared beyond the Centers. This is important information for the Regional Radio System users to have. The topography of the

region causes radio coverage fluctuations based on where a radio user is located. Having advance knowledge either before an incident occurs or during the planning stages for an event can provide response personnel with greater situational awareness and the correct communications capabilities for the site in question.

The talkpath identification process should be formalized and coordinated amongst the Dispatch Centers in the region. The information derived from this effort should be documented and distributed to the Regional Radio System user agencies for their consumption.

An additional aspect of this process should include an annual review of the site trunking and Failsoft programming each agency's radio are programmed with. This is to ensure the correct talkpaths are being designated when the Regional Radio System goes into either of these fall back modes.

Recommendations:

1. Formalize the talkpath identification process.
2. Each agency using the Regional Radio System should conduct an annual review of their radios' site trunking and Failsoft programming.
3. Document the results of the talkpath identification process.
4. Distribute the results of the identification process to the Regional Radio System user agencies.

4.10 Site Trunking and Failsoft Training

Description: Generally, first responders across the country only train with their agency radio equipment during their initial training academy. Additionally, the level of training they do receive is agency dependent and varies from extremely basic to relatively detailed. Very few agencies across the country incorporate or require annual radio training. Advanced training is virtually non-existent for line level responders. Agencies in the State of Oregon are no different.

ICTAP C/Es learned during Gremlins in the Gears that users of the Regional Radio System are not receiving training on Site Trunking and Failsoft. The Regional Radio System managers and radio technicians playing in Gremlins in the Gears expressed deep concern about these two topics. First responders that are completely unaware of what Site Trunking and Failsoft do to their ability to communicate, either locally or wide area, may be put into life threatening situations simply because they were not properly trained. It is important that users, especially first responders, become educated in the effects Site Trunking and Failsoft have on the Regional Radio System and how to recognize and respond when these system safety levels are activated. Education should be followed up with practical applications by being included in annual training and exercise regimens.

Recommendations:

1. Develop a Site Trunking – Failsoft training tool to educate users of the Regional Radio System on these topics.
2. Encourage Regional Radio System user agencies to educate their personnel on Site Trunking and Failsoft.
3. Encourage Regional Radio System user agencies to incorporate radio training into their annual training requirements.

4.11 Communications Unit Training

Description: Some of the Players taking part in the functional exercise portion of Gremlins in the Gears were not the traditional Communications Unit personnel ICTAP C/E's were expecting to play. Trained Communications Unit position holders or those in training with open position task books normally fill the Player ranks. In this exercise four Players were radio shop technicians and one Player was a Dispatch Center representative. Some of these Players had a very good understanding of the Communications Unit positions but none have taken any of the Communications Unit position courses or have open position Task Books.

The use of radio shop technicians in the Communications Unit turned out to be a positive experience for both Players and Exercise Staff. The leadership skills exhibited by the Players were exceptional. Several of the non-traditional Players expressed a desire to take Communications Unit courses and open position Task Books to complete the credentialing process. This however, was met with concern by some Observers since the radio technicians would most likely be needed at their home agency when incidents/events occurred. None of the FE Players were expecting to start the process to become credentialed Communications Unit personnel. Agencies should not dismiss the importance of having trained and credentialed Communications Unit personnel on staff in the event of an incident or preplanned event.

The State of Oregon has been proactive and successful in their Communications Unit personnel recruiting efforts and encourages agencies to designate a Communications Unit Leader (COML) early on in incidents and events. The problem is providing enough opportunities for trainees seeking full Communications Unit credentialing to get their position Task Books completed. This problem is why it is important to take full advantage of training opportunities such as Gremlins in the Gears when they arise. This is not meant to diminish the skills and excellent work the Players that did participate demonstrated. It is only to point out how this opportunity could have been beneficial to those persons seeking Communications Unit credentials.

Recommendations:

1. Continue proactive recruiting of potential Communications Unit personnel.
2. Ensure Communications Unit personnel and/or Communications Unit position trainees attend as many training events that contain a communications component as possible to support the credentialing process.
3. Continue to assign Communications Unit personnel on incident/events when needed, and when practical, assign Communications Unit position trainees to give them real world experience.
4. Continue to seek out Communications Unit training opportunities such as ICTAP drills and functional exercises as well as State and locally led exercises.
5. Continue to encourage agencies to designate a COML in incidents and events.
6. Consider including non-traditional Communications Unit personnel, such as radio technicians, for training and credentialing.

4.12 LRIG Mobile Communications Trailer

Description: The Lane Regional Interoperability Group (LRIG) mobile communications trailer was the sole Mobile Communications Unit (MCU) asset present at Gremlins in the Gears. The trailer is a work in progress but is very capable in its current configuration. A briefing was given covering the functionalities and modifications of the trailer. Some of the modifications made to the trailer will require additional labeling and safety equipment.

A large generator and separate large fuel tank have significantly increased the trailer's weight. The dry weight and loaded weight should be posted on the outside of the trailer. Weight information is needed by anyone tasked with transporting it so braking distances can be adjusted. Special attention should be paid to bridge weight limits in rural areas. The increased weight of the trailer also warrants speed limit labeling similar to those found on U-Haul trailer fenders indicating the trailer should not exceed 55 miles per hour.

The addition of a generator mandates the need to mitigate engine exhaust fumes when the generator is in use. Currently the engine exhaust pipe is only a few inches long. This does not effectively move the exhaust far enough away from the vehicle for safe operation. There are many examples of ways to facilitate the necessary mitigation on the internet. Carbon Monoxide (CO) is the harmful gas engine exhaust creates. At the time of Gremlins in the Gears the LRIG trailer did not have a CO detector installed.

The addition of the fuel tank added to the trailer requires the trailer to be properly marked with hazardous material placards. This is an important safety marking that informs those around the trailer that it contains potentially hazardous materials.

During the Hotwash discussion, the topic of MCU specification and equipment lists or quick reference cards was brought up. This type of document provides equipment owners and operators the important information about the MCU they are working with. These documents usually contain the MCU's length, height, weight, power source requirements, and capabilities such as radio caches, gateways, data, and telephone. The information can be as extensive as needed. Having this type of information readily available can reduce the amount of time owners and operators need to spend preparing and operating the MCU. This document can be adapted for use as a mission ready package detailing all the information a requestor needs to know about the vehicle, its availability, and response area. A sample MCU specification and capabilities document can be found in Appendix D of this AAR.

Recommendations:

1. Ensure the LRIG trailer is marked with its new weights and speed limitation.
2. Seek out ways to safely mitigate generator exhaust.
3. Install a CO detector in the LRIG trailer.
4. Ensure the applicable hazardous materials placards are attached to the outside of the LRIG trailer.
5. Create an LRIG mission ready package to be disseminated among area agencies.

4.13 Vendor Relationships

Description: The primary subject of Gremlins in the Gears was cybersecurity of the Regional Radio System and its components. Players expressed concern about the relationships they have with their vendors. It was not immediately clear what process is required and who they would call for quick response in the event of a cyberattack. Information about what to expect from their vendors in the event of a cyberattack regarding vendor capabilities and system vulnerabilities was not readily available either. These are important topics to be discussed by the local agencies and their vendors prior to an incident occurring. Having clear lines of communication and set expectations are an important part of a cybersecurity plan.

Recommendations:

1. Formalize vendor relations to set clear processes and expectations.
2. Document vendor processes to include in cyber-response plans.

3. Distribute documented vendor processes to local agencies as needed.
4. Develop a vendor contact list to ensure rapid communication in case of an outage.

4.14 Inclusion of Key Agencies

Description: Some key agencies with predicted roles in the fictional cyber incidents did not provide Players for the exercise. The response to the exercise scenarios as presented involved state and local agencies that did not have personnel playing at the exercise. For example, exercise participants heavily relied on vendor support to assess and diagnose the cyber incident and impact to the system. Exercise participants could therefore only simulate actions these agencies/organizations would have taken. and make assumptions regarding their roles and response protocols. In some instances, this was a result of pandemic restrictions; however, a virtual component was available to facilitate agency involvement. Additionally, the Oregon State Police, area Communications Unit trainees, and the primary radio system vendor, Motorola, would have had valuable information to contribute to the TTX and functional exercise.

Recommendation:

1. Encourage and promote participation by all key regional agencies in future training exercises so that a more realistic overall public safety response can be practiced.

4.15 ICS Training for IT and EOC Personnel

Description:

Modern day Communications Units are integrating IT personnel to support the data and IT needs of the agencies and commanders they support. EOCs are developing cyber duties under a new ESF position. It is important that IT and EOC cyber personnel have a working understanding of the National Incident Management System (NIMS) Incident Command System (ICS) format and organizational structure to effectively anticipate the needs and requirements of Incident Commanders, Section Chiefs, and other management levels of an incident or pre-planned event.

IT and EOC cyber personnel should consider taking these NIMS/ICS courses:

- IS-100.C – Introduction to the Incident Command System
- IS-200.C – Basic Incident Command System for Initial Response
- IS-700.B – Introduction to the National Incident Management System
- IS-800.D – National Response Framework, An Introduction

All of these courses can be taken online at the Emergency Management Institute (EMI) website https://training.fema.gov/emi.aspx. Other IT related courses may also be available at EMI (see section 4.2.12).

Recommendation:

1. Encourage IT and EOC cyber personnel that serve roles in incidents or pre-planned events to seek out and attend ICS courses.

4.16 Resource Request Process

Description: During large scale incidents that cause the activation of an Emergency Operations Center (EOC) certain processes and procedures are activated as well. The primary one that has the most effect on local agencies is the Resource Request process. In times of distress

Resource Requests can be fluid or held up based solely on whether the correct submission process was followed. The same is true for the EOC receiving these requests. Many times, duplicate requests come in from the same agency for the same item or requests are sent to the wrong place only to get lost in the system.

Emergency Managers have a set process for Resource Requests. This process should be documented and distributed to the agencies the EOC supports. Including the submission process, ensuring to cover the necessary information required in a request and how it is submitted, should be part of annual training. Exercises can educate and improve the accuracy of requests being made by local agencies.

Recommendations:

1. Document the EOC Resource Request process.
2. Distribute the EOC Resource Request process to local agencies.
3. Train local agencies on the Resource Request process.
4. Consider adding an EOC Resource Request component to future exercises.

4.17 GETS/WPS Awareness

Description: The State of Oregon is proactive in their promotion of the Government Emergency Telecommunications Service (GETS) for landline priority access and the Wireless Priority Service (WPS) for cellular priority. However, some participants were unaware of these services. While not ensuring communications should landline or cellular technologies totally fail, these systems could provide priority access to functioning systems for public safety personnel should the systems be operational but heavily loaded with high call volumes.

CISA has created an application that completes the necessary dialing procedure. The PTS Dialer App is available for both Android and iOS operating systems. They can be found at https://gets-wps.csgov.com/apps/.

Join your DHS CISA Region's 8 and 10, Priority Telecommunications Access Representative (PAR), the second Thursday of each month (*excluding holidays) at 1:00 PM Pacific Time for a monthly PTS Overview and Updates webinar or dial in at 1-872-240-3212, Access Code 356-294-125.

Recommendations:

1. Disseminate DHS quick reference information for the use of GETS and WPS.
2. Ensure that necessary personnel understand the various uses and applications where these resources can be applied.
3. Ensure that the capabilities and limitations of these resources are a part of any information or training provided.
4. Acquire and test GETS/WPS services. Review information at http://www.dhs.gov/publication/getswps-documents for guidance on properly testing these services.
5. Incorporate GETS/WPS into future training and exercises.
6. Ensure all permanent critical facilities (i.e., 9-1-1 Centers, EOCs, medical facilities, etc.) have GETS for all landline phones.
7. Ensure critical personnel have cell phones equipped with WPS access.
8. Ensure all necessary critical facility personnel regularly test the use of GETS cards on facility landline phones.

4.18 Telecommunications Service Priority

Description: Gremlins in the Gears focused on the loss of the Regional Radio System and PSAPs due to a cyber incident. Restoration of these pathways can sometimes be expedited by enrollment in the Telecommunications Service Priority (TSP) program[9]. TSP is a program that authorizes national security (NS) and emergency preparedness (EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. TSP service user organizations may be in the federal, state, local, or tribal governments; critical infrastructure sectors in industry; or non-profit organizations that perform critical NS/EP functions.

There are two primary uses for TSP; one for installing new service and one for restoring existing service. When circumstances require installation of a new telecommunications service faster than a service vendor's normal processes allow, an organization may request provisioning priority. This can be an immediate installation following an emergency or an installation by a specific date, also known as an essential provisioning. Restoration priority is for new or existing telecommunication services and requires that service vendors restore them before non-TSP services. Restoration priority helps minimize service interruptions that may have an adverse effect on the supported NS/EP functions. Organizations must request TSP restoration priority on its circuits before a service outage.

Recommendations:

1. Determine whether eligible lines of communication are currently enrolled in the TSP program.
2. Enroll all eligible lines of communication that are not currently enrolled in the TSP program.

4.19 General Training Recommendations

Training can make a substantial improvement to the knowledge responders possess and their ability to apply that knowledge to the incident at hand. Many of the deficiencies in performance or knowledge as displayed by responders and communication specialists during the exercise can be rectified by an increase in applicable training.

Develop a training protocol that includes the whole spectrum of emergency responders from the local to the state and federal levels. Although by no means exhaustive, some additional examples of recommended training opportunities the region could pursue include:

1. Discipline-specific communications training. Trainings of this type are available through groups such as the Association of Public Safety Communications Officials (APCO), National Emergency Number Association (NENA), etc.
2. Communications Unit position-specific training courses available through CISA/ICTAP.
    a. Communications Unit Leader
    b. Communications Technician
    c. Incident Communications Center Manager
    d. Incident Tactical Dispatcher
    e. Radio Operator
    f. Information Technology Service Unit Leader

[9] https://www.cisa.gov/about-tsp

g. Auxiliary Communications

3. Regional subject matter experts who can become instructors in applicable training topics through train-the-trainer courses.
4. Routine training opportunities such as weekly radio-net tests, etc.

The following are some online training resources:

CISA provides emergency communications tools and resources at the Safecom website (cisa.gov/safecom). This website provides:

- Communications Unit training resources (cisa.gov/safecom/communications-unit). These include the annual Communications Unit master training calendar and how to request these courses and other training through ICTAP.
- Communication Assets Survey and Mapping (CASM) (cisa.gov/safecom/casm-tool) provides a secure, free, nationwide tool for agencies to inventory, share, and plan usage of public safety emergency communications assets.

Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up-to-date on skills and evolving threats. CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation. These resources can be found at the CISA Cybersecurity Training and Exercises website: https://www.cisa.gov/cybersecurity-training-exercises.

The **FEMA Emergency Management Institute (EMI) Virtual Campus** at training.fema.gov/EMI.aspx has numerous online courses of interest, including several courses offered under the FEMA Independent Study Program such as:

- IS-100 Introduction to the Incident Command System (ICS)
- IS-700 An Introduction to the National Incident Management System (NIMS)

The **FEMA National Preparedness Directorate National Training and Education Division (NTED)** at firstrespondertraining.gov offers more than 150 courses to help build critical skills that responders need to function effectively in mass consequence events.

APCO International (apcointl.org/training-and-certification) offers telecommunicator and dispatch training.

NENA (nena.org/page/education) offers courses that span the breadth and depth of 9-1-1 technology and PSAP operations topics.

5 CONCLUSION

The Oregon Gremlins in the Gears Cybersecurity TTX/FE is an essential step toward increasing and improving communications cybersecurity throughout the State of Oregon. By continually assessing progress and making improvements, public safety entities across the state will continue to excel in their dedication to disaster preparedness and their mission to achieve an optimal level of communications cybersecurity. Their efforts to date have been exemplary and will serve the state admirably for years to come.

.

APPENDIX A IMPROVEMENT PLAN

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
Identification and Declaration of Cybersecurity Incident	Train personnel to notify a supervisor or higher authority in any instance where software or hardware is not operating as intended.					
	Train supervisors to assess and determine the type of incident (e.g., hardware failure, software flaw, cyber incident).					
	Document escalation procedures to provide guidance for declaring a cyber incident and activating incident response to include notification of interconnected system authorities.					
COOP and Disaster Recovery Plans	Update existing COOP to include response to cybersecurity incidents.					
	Update existing DR plans to comply with §403.150 and include response to cybersecurity incidents.					
	Incorporate 9-1-1 call handling procedures during cyber incidents into DR plans.					
	Incorporate COOP and DR plans into future training and exercises.					
Cybersecurity Awareness Training	Develop cybersecurity awareness training for users, technicians, and supervisors with specialized training for those in administrative or supervisory positions.					

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
	Provide cybersecurity awareness training for all users of all systems.					
	Provide advance cybersecurity training for those personnel whose position or duties dictate.					
IT Account Control	Develop or update existing Cyber Standard Operating Procedures (CSOP) for configuring and operating information system account privileges.					
	Train personnel on CSOPs as part of the cyber awareness training.					
	Apply CSOPs to systems from the very beginning, even during buildup and testing phases.					
Dependence on Vendors for Security	Review current SLAs with infrastructure vendors to ensure those agreements address the cybersecurity requirements described above.					
	Consider the cybersecurity requirements described above in future SLA negotiations.					
System Notifications and Coordination	Document when escalation procedures are implemented, declaring a cyber incident and activating incident response to include notification of interconnected system authorities.					
	Develop separate communication plans to inform/involve the technical staff from all the IT groups supporting the system and the radio technicians.					

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
	Continue using the Oregon Emergency Response System (OERS) mechanism for resource requests but also add another level of notifications to cyber or communications representatives to allow for quicker response.					
	Coordinate with any network connected entities to align cyber policies					
Command and Control of Tech Related Incidents	Cross train radio technician personnel in the IT Major Incident Process and the Incident Manager position.					
	Consider using a Unified Command type response, consisting of communications and IT personnel when the Regional Radio System suffers a cyber incident.					
	Create a commonality of terms quick reference card listing the terms used by IT and Communications Technicians.					
Personnel Redundancy	Consider implementing a mentoring program for key system support personnel.					
	Consider implementing a shadowing program for potential successors of key personnel.					
	Consider developing formal documentation for contacts and procedures to address radio system problems so that the system is not reliant on informal institutional knowledge of a limited number of people.					

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
Formalized Talkpath Functionality Documentation	Formalize the talkpath identification process.					
	Each agency using the Regional Radio System should conduct an annual review of their radios' site trunking and Failsoft programming.					
	Document the results of the talkpath identification process.					
	Distribute the results of the identification process to the Regional Radio System user agencies.					
Site Trunking and Failsoft Training	Develop a Site Trunking – Failsoft training tool to educate users of the Regional Radio System on these topics.					
	Encourage Regional Radio System user agencies to educate their personnel on Site Trunking and Failsoft.					
	Encourage Regional Radio System user agencies to incorporate radio training into their annual training requirements.					
Communications Unit Training	Continue proactive recruiting of potential Communications Unit personnel.					
	Ensure Communications Unit personnel and/or Communications Unit position trainees attend as many training events that contain a communications component as possible to support the credentialing process.					

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
	Continue to assign Communications Unit personnel on incident/events when needed, and when practical, assign Communications Unit position trainees to give them real world experience.					
	Continue to seek out Communications Unit training opportunities such as ICTAP drills and functional exercises as well as State and locally led exercises.					
	Continue to encourage agencies to designate a COML in incidents and events.					
	Consider including non-traditional Communications Unit personnel, such as radio technicians, for training and credentialing.					
LRIG Mobile Communications Trailer	Ensure the LRIG trailer is marked with its new weights and speed limitation.					
	Seek out ways to safely mitigate generator exhaust.					
	Install a CO detector in the LRIG trailer.					
	Ensure the applicable hazardous materials placards are attached to the outside of the LRIG trailer.					
	Create an LRIG mission ready package to be disseminated among area agencies.					
Vendor Relationships	Formalize vendor relations to set clear processes and expectations.					

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
	Document vendor processes to include in cyber-response plans.					
	Distribute documented vendor processes to local agencies as needed.					
	Develop a vendor contact list to ensure rapid communication in case of an outage.					
Inclusion of Key Agencies	Encourage and promote participation by all key regional agencies in future training exercises so that a more realistic overall public safety response can be practiced.					
ICS Training for IT and EOC Personnel	Encourage IT and EOC cyber personnel that serve roles in incidents or pre-planned events to seek out and attend ICS courses.					
Resource Request Process	Document the EOC Resource Request process.					
	Distribute the EOC Resource Request process to local agencies.					
	Train local agencies on the Resource Request process.					
	Consider adding an EOC Resource Request component to future exercises.					
GETS/WPS Awareness	Disseminate DHS quick reference information for the use of GETS and WPS.					
	Ensure that necessary personnel understand the various uses and applications where these resources can be applied.					
	Ensure that the capabilities and limitations of these resources are a part of any information or training provided.					

Capability/Gaps	Recommendations	Corrective Action	Primary Responsible Agency	Agency POC	Start Date	Completion Date
	Acquire and test GETS/WPS services. Review information at http://www.dhs.gov/publication/getswps-documents for guidance on properly testing these services.					
	Incorporate GETS/WPS into future training and exercises.					
	Ensure all permanent critical facilities (i.e., 9-1-1 Centers, EOCs, medical facilities, etc.) have GETS for all landline phones.					
	Ensure critical personnel have cell phones equipped with WPS access.					
	Ensure all necessary critical facility personnel regularly test the use of GETS cards on facility landline phones.					
Telecommunications Service Priority	Determine whether eligible lines of communication are currently enrolled in the TSP program.					
	Enroll all eligible lines of communication that are not currently enrolled in the TSP program.					

APPENDIX B EXERCISE PLANNING TEAM

Table B-1: Exercise Planning Team Contact List

Name	Agency / Department	Email Address	Phone
Aaron Fox	Washington County Emergency Management / Oregon SIEC Technology Committee	aaron.fox@portlandoregon.gov	503-793-2196
Brian Craig	CISA/ICTAP	brian.h.craig@saic.com	402-290-5004
Brian Greig	Lane County Technology Services	brian.greig@lanecountyor.gov	
Cinnamon Albin	Cyber Security Services - State of Oregon	cinnamon.s.albin@oregon.gov	503-373-1496
Dana Lockhart	CISA Region 10	dana.lockhart@cisa.dhs.gov	425-903-0217
David Adsit	CISA/ECD	david.adsit@cisa.dhs.gov	202-948-3411
Dennis Alexander	City of Eugene, South West 7 Counties System Administrator	dennis.w.alexander@ci.eugene.or.us	
Harlan Squires	CISA/ICTAP	harlan.t.squires@saic.com	760-473-3034
James Jarvis	CISA	james.jarvis@cisa.dhs.gov	202-834-0631
Jeremy O'Leary	Multnomah County	jeremy.oleary@multco.us	503-314-8316
Josh Rue	Linn County Sheriff's Office	jrue@linnsheriff.org	
Les Defoor	Oregon SOC	les.defoor@das.oregon.gov	503-480-6709
Michael Harman	Lane County Technology Services (Radio System Manager)	michael.harman@lanecountyor.gov	541-682-4384
Oscar Parsons	DAS/EIS Interoperability	oscar.parsons@das.oregon.gov	503-378-8054
Ric Lentz	Linn County Sheriff's Office	rlentz@linnsheriff.org	
Robert Quinn	Multnomah County	robert.quinn@multco.us	503-307-4129
Sarah Shelton	Linn County Sheriff's Office	sshelton@linnsheriff.org	541-917-6660
Theresa A. Masse	CISA	theresa.masse@cisa.dhs.gov	503-930-5671
William Chapman	Statewide Interoperability Program	william.chapman@oregon.gov	971-283-4607

APPENDIX C EXERCISE PARTICIPANTS

Table C-1: Exercise Participants Contact List

Last	First	Agency/Department	Email	Role	TTX	FE
Albin	Cinnamon	Cyber Security Services - State of Oregon	cinnamon.s.albin@oregon.gov	Observer	x	
Chandler	Robert	City of Eugene, Public Works Radio Shop	rchandler@eugene-or.gov	Player	x	x
Chapman	William	Statewide Interoperability Program	william.chapman@oregon.gov	Evaluator	x	x
Craig	Brian	CISA/ICTAP	brian.h.craig@saic.com	Facilitator	x	x
Crawford	Jessica	City of Springfield, Oregon	jcrawford@springfield-or.gov	Player	x	x
Davis	Elijah	Lane County	elijah.davis@lanecountyor.gov	Observer	x	x
Dorman	Wayne	Eugene Police	wdorman@eugene-or.gov	Player	x	
Dunlap	Brad	Lane County Sheriff's Office	bradley.dunlap@lanecountyor.gov	Player	x	x
Fox	Jason	CISA/ICTAP	jason.w.fox.civ@us.navy.mil	Observer	x	x
Fox	Aaron	Washington County Emergency Management	tenukifox@gmail.com	Observer	x	x
Franklin	Andy	Linn County Sheriff's Office	afranklin@linnsheriff.org	Player	x	x
Greig	Brian	Lane County Technology Services	brian.greig@lanecountyor.gov	Observer	x	x
Harman	Michael	Lane County IT	michael.harman@lanecountyor.gov	Player	x	x
Hugi	Robert	CISA/ECD	robert.hugi@cisa.dhs.gov	Observer	x	x
Kemp	Jason	Adcomm Engineering	j.kemp@adcomm911.com	Observer	x	x
King	Stephen	Central Lane 9-1-1	skingbeyone-or.gov	Player	x	x
Lentz	Ric	Linn County Sheriff's Office	rlentz@linnsheriff.org	Observer	x	x
Machado	Maurice	Lane County	maurice.machado@lanecountyor.gov	Player	x	x
Masse	Theresa	CISA	theresa.masse@cisa.dhs.gov	Observer	x	x
Mele	Adam	Oregon Department of Justice / TITAN Fusion Center	adam.t.mele@doj.state.or.us	Observer	x	
Miller	Michelle	Springfield Police Department	mmiller@springfield.or.gov	Player	x	
Nesselrode	Derek	CISA/ECD	derek.nesselrode@cisa.dhs.gov	Observer	x	
Noel	Steve	CISA	steven.noel@cisa.dhs.gov	Observer	x	
O'Leary	Jeremy	Multnomah County	jeremy.oleary@multco.us	Online Observer	x	
Oster	Eric	Lane County	eric.oster@lanecountyor.gov	Online Player	x	
Parsons	Oscar	Enterprise Information Services - Shared Services - Statewide Interoperability	oscar.parsons@das.oregon.gov	Online Observer	x	
Perkins	Joshua	Linn County Sheriff's Office	jperkins@linnsheriff.org	Player	x	x
Perry	Richard	City of Eugene	rperry@eugene-or.gov	Player	x	x
Poiner	Robert	Central Lane 9-1-1	rpoiner@eugene-or.gov	Observer	x	x

Last	First	Agency/Department	Email	Role	TTX	FE
Ray	Jeremy	City of Eugene Radio Shop	jray@eugene-or.gov	Player	x	x
Ronning	Susan	Adcomm Engineering	s.ronning@adcomm911.com	Observer	x	x
Rue	Josh	Linn County Sheriff's Office	jrue@linnsheriff.org	Observer	x	x
Scarci	Patricia	City of Eugene (Information Technology)	pscarci@eugene-or.gov	Online Player	x	
Shelton	Sarah	Linn County Sheriff's Office	sshelton@linnsheriff.org	Observer	x	x
Silva	Reuben	ODHS EMU	reuben.s.silva@dhsoha.state.or.us	Player	x	x
Smith	Brandon	CISA/ECD	brandon.smith@cisa.dhs.gov	Observer	x	x
Squires	Harlan	CISA/ICTAP	harlan.t.squires@saic.com	Facilitator	x	x
Vogeney	Kenneth	City of Springfield, Oregon	kvogeney@springfield-or.gov	Player	x	
Wallace	Lisa	CISA/ICTAP	lisa.wallace@echoorigin.com	Evaluator	x	x
White	Andrew	CISA/ICTAP	awhite@lafayettegroup.com	Evaluator	x	x
Wilson	Christina	CISA/ICTAP	christina.l.wilson@saic.com	Evaluator	x	x

APPENDIX D MCU SPECIFICATIONS AND CAPABILITIES

Below is an example of an MCU specifications and capabilities document.

Mobile Unit		
Agency		
Unit Name/#		
POC Name:	***Cell #:***	
Mobile Unit Specifications		
Length		[Insert MCV Picture]
Self-propelled MCU/MCV, or requires tow vehicle, other related support vehicles or logistics/equipment trailers, etc. that must remain with the MCU		
MCU horizontal clearance/footprint/parking space requirements		
Type, maximum height, and wind rating of any extendable antenna mast(s)		
Both MCU engine and generator fuel type		
Capabilities	**Amount**	**Type**
Mobile Radios		
Cache Radios		
Gateway		
Mobile Relays/Repeaters		
Data Terminals		
Internet Connectivity		
Email Address		
Phone Number/type (cell, iridium, landline, etc)		
Satellite		
Fax		
Surveillance		
Amateur Radio Equip		
Auxiliary Power		
Other:		

APPENDIX E OREGON CSS QUICK SHEET

Oregon Cyber Disruption Response & Recovery - Voluntary Resource Guide for Local Government
Quick Sheet

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

Oregon Cyber Disruption Response & Recovery - Voluntary Resource Guide for Local Government
Quick Sheet

CONTACT LIST

Cyber Disruption Notification

When to Notify

If you are experiencing a cyber disruption, notifying CSS is recommended, whether you need assistance or not. Notification can occur at various stages, even when complete information is not available. Notification allows correlations of cyber events across the state to identify coordinated attacks or attack trends, access to mitigation measures and expertise from similar attacks, and cyber response support.

Who to Notify

Cyber Security Services Security Operations Center
Email: eso_soc@oregon.gov
Phone: 503-378-5930

Additional Notification Resources

Cybersecurity and Infrastructure Security Agency (CISA)
Theresa A. Masse
Cyber Security Advisor, Region X (Oregon)
Email: theresa.masse@cisa.dhs.gov
Mobile: 503-930-5671

MS-ISAC -The Security Operations Center (SOC) is available 24/7 to assist via phone or email:
soc@cisecurity.org
Phone: 866-787-4722

What to Report

Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified. Situational Awareness - CSS may share de-identified information with Trusted Partners for situational awareness. Trusted Partners are OEM, Titan Fusion Center, MS-ISAC, CISA, and National Guard

APPENDIX F GLOSSARY

AAR	After Action Report
APCO	Association of Public Safety Communications Officials
CASM	Communication Assets Survey and Mapping
C/E	Controller/Evaluator
CISA	Cybersecurity and Infrastructure Security Agency
CO	Carbon Monoxide
COML	Communications Unit Leader
COOP	Continuity of Operations
CSOP	Cyber Standard Operating Procedures
CSS	Cyber Security Services
DAS	Department of Administrative Services
DHS	Department of Homeland Security
DR	Disaster Recovery
ECD	Emergency Communications Division
EIS	Enterprise Information Services
EMI	Emergency Management Institute
EOC	Emergency Operations Center
EP	Emergency Preparedness
EPT	Exercise Planning Team
ESF	Emergency Support Function
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
HSEEP	Homeland Security Exercise Evaluation Program
ICS	Incident Command System
ICTAP	Interoperable Communications Technical Assistance Program
IP	Improvement Plan
IS	Independent Study
IT	Information Technology
LRIG	Lane Regional Interoperability Group
MCU	Mobile Communications Unit
MFA	Multi-Factor Authentication
NENA	National Emergency Number Association
NIMS	National Incident Management System
NS	National Security
NTED	National Training and Education Division
OERS	Oregon Emergency Response System
PACE	Primary, Alternate, Contingent, Emergency
PPD	Presidential Policy Directive
PSAP	Public Safety Answering Point

RAN	Radio Access Network
SIEC	State Interoperability Executive Council
SLA	Service Level Agreement
SOC	Security Operations Center
SOP	Standard Operating Procedure
SWIC	Statewide Interoperability Coordinator
TCL	Target Capability List
TSP	Telecommunications Service Priority
TTX	Tabletop Exercise
VLAN	Virtual Local Area Network
WPS	Wireless Priority Service