EMERGENCY SUPPORT FUNCTION #2 - COMMUNICATIONS

RESPONSE PLANNING FUNCTION

_____
Michael Mattmiller, Chief Technology Officer,
Director Seattle Information Technology
Department

1/25/17
_____
Date

_____
Barb Graff, Emergency Manager

1/26/17
_____
Date

Note: This ESF is part of the Response Planning Function from the Comprehensive Emergency Management Plan and this version includes the 2016 updates. Seattle Information Technology Department acts as the current ESF Coordinator and collaborated with many partners for respective updates.

TABLE OF CONTENTS

TABLES

FIGURES

No table of figures entries found.

1. STAKEHOLDERS

Table 1

PRIMARY DEPARTMENT	ESF COORDINATOR
Seattle Information Technology Department	Seattle Information Technology Department

Table 2

SUPPORT DEPARTMENT AND AGENCIES	
Auxiliary Communications Services (Seattle EOC)	City of Seattle Departments

2. INTRODUCTION

2.1 Purpose

Electronic communications and information technology are a vital component to preventing, preparing for, responding to, and recovering from disasters, both natural and results of terrorist acts. This annex describes the technology and telecommunications support the City of Seattle's capabilities, and how those capabilities will be managed during time of disaster.

2.2 Scope

- This annex applies to the departments, organizations or agencies with a lead or support role for this ESF. It discusses the requirements, business approach, and objectives of ESF #2 communications role and information technology including programs and operations before, during, and after a major emergency or disaster.
- The Seattle Information Technology Department (ITD) is charged with management, operations, and maintenance for the majority of the City government's telecommunications and information technology infrastructure. ITD is responsible for coordinating operational services for the telecommunications and information technology infrastructure.
- Application support for almost all of the IT applications (e.g. computer-aided-dispatch, work management) used in City government resides currently in the owning / using department; and all these applications are dependent upon the information technology infrastructure being operational.
- ITD's Department Director has the additional responsibility as the Chief Technology Officer for the City, and, as such, sets standards which all departments are expected to follow when acquiring and implementing technology and telecommunications. During, cybersecurity incidents, disasters, and EOC activations, the CTO and the CTO's designees in the EOC direct the activities and coordination with other departments, which support telecommunications and information technology for City government.
- At this time, Seattle Information Technology Department coordinates the Public Safety Radio network for the region. The Seattle radio network is a part of a linked and jointly operated King County region wide network of more than 14,000 radios used by all police and fire agencies in King County.

3. SITUATION

3.1 Emergency Conditions and Hazards

- Hazards facing Seattle are well-described in the document Seattle Hazard Identification and Vulnerability Analysis. The information below supplements that plan with certain specifics relevant to telecommunications and information technology. Communications have been developed to support all components of response and recovery plans and redundancies have been provided in case of failure of primary systems.

- All disasters. During any major disaster in the region, the region's normal communications networks will be overloaded – these are the public switched telephone network (PSTN) and cellular telephone networks. Generally, the City's internal telephone, radio and data networks are segregated from the public networks and will operate normally. Normal traffic is designated for internal government traffic; exceptions would be out-dialing or inbound traffic from outside the City. Generally, the PSTN and public cell phone networks will continue to operate, but only a small percentage of telephone calls will be connected. City employees may continue to try and use the cellular network for low-priority and non-emergency communications. City employees should use e-mail functions of their smart phone and similar devices and the text messaging features of their cellular phones which should continue to operate, although somewhat slowed during the initial stages of the disaster.

- Earthquake. When an earthquake occurs, the ground motion will potentially continue for some time. All critical radio IT assets (servers, radio transmitters, etc.) are earthquake braced and generally in modern facilities built to withstand most anticipated earthquakes. A serious earthquake, however, could damage some interconnection paths for networks (e.g. microwave, fiber optic cable). The City's network designs include multiple redundant paths and technologies such as SONET and microwave with self-healing rings for critical sites. This design concept will help ensure service is available. ITD has completed building out a secondary data center site with all redundant critical infrastructure systems in place. This will provide the City with a fully operational data center in response to earthquake damage within the City of Seattle and help in recovery of critical information technology systems. The primary data center site and the secondary data center have equipment located on base isolation pads. The buildings containing the data centers have full seismic retrofits and advanced security features with robust generator support.

- Cybersecurity Incident. Cybersecurity incidents vary in nature, complexity, and impact and include computer viruses and malware, ransomware, theft and corruption of data and system and network penetration and denial of service attacks. The nature of systems and technology subject to such incidents is increasingly complex and vast, including City-controlled computers and networks as well as mobile phones, networked devices, sensors, and third party services. ITD has a separate cybersecurity incident response plan administered by the City's Information Security Office. This plan is designed to identify, mitigate, and respond to real threats and is reviewed and exercised several times a year. These incidents do not require EOC activation. However, a truly significant cybersecurity incident adversely affecting the control systems for the City's critical infrastructure, for example, would require EOC activation to address the physical and operational effects of the incident.

- Cybersecurity incident coupled with terrorist attack. It is possible that a terrorist attack (such as a CBRNE event) could be coupled with a cybersecurity incident adversely affecting the City's information technology systems, assets, operations, and/or infrastructure. Such incidents will require activation of the EOC to deal with the physical and operational incident and the City's

Seattle
Office of Emergency
Management

CITY OF SEATTLE CEMP
EMERGENCY SUPPORT FUNCTION #2 - COMMUNICATIONS
SITUATION

cybersecurity incident response plan to address the systems, technology, and data. The TOPOFF2 exercise in 2003 exercised the plans for such a combined attack.

3.2 Planning Assumptions

- As stated before, Seattle Information Technology Department (ITD) is charged with management, operations, and maintenance for the majority of the City government's telecommunications and information technology infrastructure. ITD is responsible for helping ensure operational service for the telecommunications and information technology infrastructure. ITD will rely on their department operating center the Information Technology Operating Center (ITOC) to assist in coordination of IT resources during response to an event.

4. CONCEPT OF OPERATIONS

4.1 Organization

- The EOC is organized using Incident Command System which emphasizes concepts such as unity of command/coordination, modular organization, management by objectives, manageable span of control, etc. Under EOC Operations are four branches; Police, Fire, Human Services and Infrastructure.
- The Seattle Information Technology Department's ESF #2 Coordinator staffs the Infrastructure Branch Director position if the disaster is cybersecurity incident; in other incidents the position supports the Infrastructure branch for communications and information technology services.
- ESF #2 works closely with the other organizations and with outside private service providers for cell services.
- During an EOC activation Information Technology Operating Center (ITOC) in coordination with the ESF #2 Coordinator assigns IT resources from the Seattle Information Technology Department in response to repair infrastructure services.
- The Seattle Information Technology Department supports the computer infrastructure components that provide emergency notification of staff and the public. These altering systems include a primary channel for the City's externally hosted WordPress blog (Alerts.Seattle.gov). Other notification systems that are also supported by the computer infrastructure include the Emergency Notification System (ENAS) and various blog sites. These systems will be fully described within the Alert and Warning Annex.

4.2 General Response

- At the time the EOC is activated, the ESF #2 Coordinators and ITD Executive Team will be notified.
- The four designated respondents to the EOC for the ESF #2 Coordinators will coordinate among themselves to determine who will report and who will relieve the reporting individual.
- The ESF#2 Coordinator will call in any additional roles that are required such as resources from Seattle Channel or the Web Support team.
- Seattle Information Technology Department's Director in coordination with the ITD Executive Team and the ESF #2 Coordinator will decide whether to activate the Information Technology Operation Center (ITOC) and will communicate their decision to the ITOC Operating Center Manager.
- As each on-call or EOC-reporting employee arrives at the EOC or a designated location, that employee will determine the status of technology systems, and will report the status of those systems to the ITOC Operating Center Manager. Priority of systems for status determination and repair are the following list:
  - 800 MHz Public Safety Radio network; Wireless data network for first and second responders; Telephone network; Public Safety (SPD and SFD); Data communications network including fiber; E-mail and messaging; City's Internet connection; City's website (seattle.gov); City's television channel (Seattle Channel).
- After ascertaining the status of the City's IT assets and networks, the ITOC Operating Center Manager will coordinate with the ESF 2 coordinator at the EOC and designate the priority for restoring IT networks and systems. The ITOC Operating Center Manager will work with other appropriate employees and supervisors to direct resources as required.

- Once ITD employees reporting to the EOC have established the complete operation of technology systems, the ITOC Operating Center Manager can release those employees for other work restoring or maintaining critical IT networks and systems.

4.3 Public Safety Radio System Interoperability and System Redundancies

- Seattle Information Technology Department coordinates the Public Safety Radio network for the region. The Seattle radio network is a part of a linked and jointly operated King County region wide network of more than 14,000 radios used by all police and fire agencies in King County. There have been numerous system redundancies designed within the Public Safety Radio network to provide alternative means of communications in the case of failure of the primary system. These systems redundancies are described within Section 6. Resource Requirements table.
- An overall Tactical Interoperable Communications Plan (TICP) was established in 2005 and updated to specifically address system interoperability changes within the Public Safety Radio network. The TICP is for the Seattle Urban Area which includes King, and Snohomish Counties and the portions of Pierce County that are serviced by Tacoma Regional Network. This plan is intended to document what interoperable resources are available within the urban area, who controls each resource and what rules of use or operational procedures exist for the activation and deactivation of each resource. The TICP is used for interoperable operational communications across jurisdictions, disciplines, and various responder levels. This plan is developed to communicate both internally and externally with all Emergency Management Program stakeholders and emergency personnel while meeting the requirements of the National Incident Management System requirements. Radio system interoperability has been addressed in design of the network, development of the operating procedures and throughout the TICP Plan.
- In addition to the Public Safety Radio network there are several City departments (Seattle City Light and Seattle Department of Transportation) radio networks that provide additional radio communications system network capabilities to provide communications specifically to support departments operations in response to a disaster or other event.
- Regional radio caches have been developed. These caches have been used across the urban area for various activations including the landslide in Snohomish County in 2013.
- The Seattle urban area including Washington State Patrol has created COML lists that are shared across the region. This aids in faster radio patching capability during an event.

4.4 Direction and Control

- The direction and control for the ESF #2 in the field will be coordinated through the Information Technology Operating Center (ITOC) which is led by Seattle Information Technology Department. This operating center in coordination with the ESF #2 coordinator located at the EOC is responsible for all information technology direction and control in the field during a disaster or other EOC activation.

4.5 Procedures

- Detailed procedures, departmental plans, and other documentation are kept in hard-copy at the EOC, shared drive within the department, and a SharePoint site location which all staff have rights and viewing capabilities.

5. RESPONSBILITIES

5.1 Prevention and Mitigation Activities

- A detailed listing of the actions to eliminate or reduce the degree of long-term risk to life, property, and the environment to be taken by the departments, organizations or agencies with a lead or support role for this ESF. Many areas needing mitigation will be identified during the preparedness, response, and recovery phases of emergency management.

- All City departments need to update their respective department Continuity of Operations Plans (COOP) so that the City's critical services are identified and the information technology systems and applications which are critical to operations are also identified. The systems and applications should have recovery time objectives listed as well as recovery point objectives. Each element is critical to be able to plan for system recovery and mitigation of the risk associated with losing the system.

5.2 Preparedness Activities

- The ESF #2 lead role is to develop a command and control structure that when activated will ensure continuity of operations for telecommunications and information technology in support of the City government. The response activities section fully describes the structure that has been established. Activation of this structure during exercises and activations has increased overall preparedness within the various duty positions.

5.3 Response Activities

- Upon a EOC activation, or whenever otherwise directed by the Emergency Operations Center Director, or the Chief Technology Officer, the following command and control structure will activate to insure continuity of operations for telecommunications and technology in support of the City government. See Table 3 below which describes position responsibility.

- The Radio & Communications Infrastructure Manager will ascertain the proper reporting location based on the nature of the disaster. Some technical analysis and configuration of the radio system can only be supported from the radio network master site.

- As many community members rely on non-verbal communication or have limited English skills, the City of Seattle will deliver key messages via Web and Seattle Channel, in a timely manner, to as many language groups as possible based on the City's Inclusive Outreach & Public Engagement (IOPE) practices and consistent with Title II of the Americans with Disability Act.

5.4 Recovery Activities

- The department will provide recovery activities for the various information technology operational components, which are defined in (Section 6. Resource Requirements). The description defines the specific scope of recovery responsibility for the Seattle Information Technology Department. The support and maintenance section defines the support and maintenance for specific components that affect city-wide information technology operations.

Table 3

EOC Reporting Matrix for IT Support			
Duty Position	**Duty Location**	**Responsibilities**	**Designees**
ESF #2 coordinator	EOC	ESF #2-Communications coordinator for the coordinating activities of ITD resources supporting telecommunications and IT during the disaster to support EOC missions	IT Strategic Advisor Deputy Chief Technology Officer Director of Engineering & Operations Sr. Manager, Network & Communications Technologies
Radio & Communications Infrastructure Manager	EOC or Radio Network Master Site or designated location	Monitor and reconfigure the public safety radio network as required to keep it operational during the disaster	Radio & Communications Infrastructure Manager
Radio Technician	EOC or Radio Network Prime Site	Monitor and reconfigure the public safety radio network as required to keep it operation during the disaster	Radio Technicians (2)
Citywide PIO Team Responder	EOC	Participate in City PIO team activities at EOC	ITD Public Information Officer
Public Information	EOC	Update the City's web	Web Manager
Technology Support (Web Team Responders)	Virtual	Sites (external and internal) with relevant information at the direction of the City's PIOs	Web Developer Web Content Designer
Web Server Administrator	Virtual	Check status of web servers.	Web Administrators
Seattle Channel Media Relations	EOC or Seattle Channel Studio	Manage the broadcast--live or taped television from the EOC or other locations with information from the EOC incident commander, Mayor or other elected official or designees.	Seattle Channel Managers (2)
Seattle Channel Headend	Seattle Channel	Manage Seattle Channel end of EOC needs	Seattle Channel Staff (2)

EOC Reporting Matrix for IT Support			
Seattle Channel EOC Television Operators	Seattle Channel	Perform television operations related to camera operations.	Seattle Channel Staff (5)
ITOC Operations Center Manager	ITOC Operating Center, Seattle Municipal Tower	Responsible for coordinating with ESF #2 coordinator to determine how to direct ITD resources as required. Prepare IT operational status reporting.	Sr. Manager Compute Systems Technologies Manager IT Operations Support Manager End User Support
ITD Director	ITD Offices, Seattle Municipal Tower	Insures accountability and safety for all ITD personnel immediately after disaster occurs. Designates and deploys channels to communicate with ITD employees throughout the duration of the disaster.	Chief Technology Officer Senior Human Resources Manager
EOC Technology Support Staffing	EOC	Report to the EOC and immediately ascertain the status of all critical technology assets necessary to support EOC functioning. Repair systems or assist EOC responders as required. These employees will be released from the EOC by the ESF #2 coordinator once the systems are determined to be operational.	Desktop Computer Support Staff, Telephone Technician (1) Data Communications Technician (1) Managers (2) On-call system engineers: Web Servers/Active Directory, Messaging/Directory, Batch Processing (CCRS)

6. RESOURCE REQUIREMENTS

The City's communications infrastructure has the following components that are critical asset requirements for the City of Seattle.

Table 4

City Communications Infrastructure		
Component	**Description**	**Support and Maintenance**
Microwave	Infrastructure connecting a few locations – largely radio transmission sites – King Countywide backbone for 800Mhz radio network but also carries some telephony and data.	First and second level support by ITD communications shop. SCL maintains some independent links. Vendors: Harris, for equipment and remote technical support.
Fiber	Over 550 miles of fiber optic cable reach every major and many smaller City facilities, including most fire stations, police precincts, libraries and schools. Backbone for telephone and data communications networks, plus some radio transmissions and traffic signals. Fiber network also supports numerous other public agencies including UW, Seattle Community Colleges, Seattle Public Schools, King County, KC Metro Transit, NOAA, FBI, US Coast Guard, WSDOT, and connections between the WA State EOC and EOC's in King, Pierce, and Snohomish Counties.	Engineering and first-level support by ITD communications shop and ITD Network Engineering & Operations. Electronics support by ITD. Fiber construction and repair by contractors under ITD management. SCL installs and maintains a connected network for electric network management. SDOT installs and maintains a connected network for traffic management purposes. Vendors: Netversant and Powercom for installation, repair. Qwest/Fujitsu for SONET equipment and remote technical support.
Radio – 800 MHz Public Safety	Seattle operates a Motorola Smartzone radio network with 7 transmission sites and about 4400 mobile and portable radios used by Police, Fire, Public Utilities and others. 25 simulcast frequencies and hundreds of talk groups. Three levels of redundancy: trunked operations, site trunking, failsoft. The Seattle network is a part of a linked and jointly operated King County region wide network greater than 14,000 radios used by all police and fire agencies in the County.	First and second level support by ITD communications shop both for the King County region-wide network and the Seattle portion of the network. Vendors: Motorola, for equipment and remote technical support.
Radio – TRIS	TRIS is the Tri-County Radio Interoperability System. TRIS was implemented in 2005 using a	First and second level support by ITD communications shop.

City Communications Infrastructure		
	combination of federal funds and urban area security initiative funds. TRIS allows some public safety answering points (PSAPs) to patch talk groups between these radio networks in the urban area: King County 800 MHz trunked, Snohomish Emergency Radio System (SERS), Tacoma 800 MHz radio, Port of Seattle 800 MHz radio, Washington State Patrol, and the Federal Integrated Wireless Network (IWN) which supports a number of DOJ and DHS agencies, including FEMA.	
Interoperable Communications Van	The Seattle Police Department acquired a communications van in 2005 which allows for interoperable wireless communications at an incident site. The wireless communications include multiple radio networks used by most government agencies operating in Seattle, interoperable switched using an Infinimode© switch. The van also has Wi- Fi, video and other capabilities.	First and second level support by ITD communications shop. ITD End User Support is responsible for Wi-Fi, and video capabilities.
Communications and command vehicles	Seattle Fire has a mobile command and communications vehicle. Seattle Police has multiple mobile precincts (command vehicles). These mobile command posts have both communications capabilities with radio, and computer/printer assets.	First and second level communications support by ITD communications shop. Information technology assets supported by Police, Fire, and ITD information technology professionals.
Radio – 800 MHz SCL	Seattle City Light operates a four-channel radio network used by SCL crews and other operations. The network is active both in Seattle and the Skagit valley. About 400 mobile and portable radios.	First and second level support by SCL staff. Vendors: Motorola, for equipment and remote technical support.
Radio – 440 MHz Amateur radio and 462 MHz GMRS radio, Emergency Management	The Seattle EOC support volunteer radio system operated as auxiliary communications networks. These include a network of 146 and 440 MHz amateur radio repeaters, as well as a network of 462 MHz GMRS repeaters.	First and second level support by volunteers through the EOC. Support is provided through the ITD communications shop on an as-requested basis. Vendors: Motorola, for equipment and remote technical support.
Radio – 450 MHz Transportation	Seattle transportation operates a 450 MHz radio network for transportation crews with about 400 mobile and portable radios.	An SDOT employee oversees the system and does some first- level maintenance. Most installation and maintenance is accomplished by contractors. Vendors:
Radio - various	Various other special-purpose radio networks	Employees in the departments

City Communications Infrastructure		
	are installed and operated by various departments. Examples: Public utilities operate a low-band network in its watersheds, and the Zoo has an UHF radio network for use on Zoo grounds.	oversee contractors who maintain, and install these networks.
Telephone Network	The City operates a private telephone network composed of 18 PBX switches, and over 12,000 telephone instruments (TDM and VoIP) based in about 300 City business locations. This system is used internally to City government and is designed to operate even when the public and cellular networks are inoperative. The network operates largely on the City's own fiber optic cable network, but also uses City-owned copper cable plant, leased circuits and data network infrastructure. A number of related services are maintained including automatic call distribution systems (ACD), interactive voice response systems (IVR), voicemail and others and cellular networks are inoperative.	First and second level support by ITD Telecommunication Engineering & Operations. Copper cable supported by ITD cabling Vendor: Nortel equipment supplied by several distributors, e.g. CenturyLink, Shared Technologies Nortel provides remote technical support.
Telephone Network Interconnection to Local and Long Distance carriers	The City maintains connections to the private telephone network (PSTN) through two local PSTN carriers CenturyLink and Level-3. These connections are via central office trunks with connections between the carrier facilities and the City's PBXs. Long Distance Service is provided via CenturyLink and Level-3 telephone. All Local trunks are provided by CenturyLink and Level-3 via Leased circuits. Circuits provided by Level-3 are delivered out of Level-3's Central Office via the City's SONET network.	First and second level support by ITD Telecommunication Engineering & Operations. Carrier service support provided by: CenturyLink, XO Communications, Level 3. Circuit support provided by CenturyLink, Level-3 and ITD Telecommunication Engineering & Operations. Avaya provides remote access technical support for PBX equipment
Data Communications	The City operates a private data communications network which links all desktop, server, mid-range and enterprise computers in City government, as well as many other special purpose services such as printers and video. The network operates largely on the City's fiber optic cable network between buildings and intra-building risers and copper for distribution within buildings. This data network is the basis for a wide variety of computer applications used for emergency	First and second level support by ITD Network Engineering & Operations.

City Communications Infrastructure		
	management, including electronic mail, computer aided dispatch, work management systems, etc.	
Internet connection	The City provides internet connections through two internet service providers (ISP). Circuit connections are routed over fiber.	First and second level support by ITD Network Engineering & Operations Vendors: Western Data Center (WDC)---Cogent and Zayo; Eastern Data Center (EDC)—Level-3 and Zayo; Guest Wireless—Cogent and Comcast
Wireless data network— Internal City wireless access points	The City provides Wireless Access Point (WAP) service in many conference rooms of Seattle Municipal Tower (SMT), Seattle Justice Center (SJC) and City Hall as well as other strategic sites in the City.	First and second level support provided by ITD Network Engineering & Operations. Vendor support provided by Cisco on a remote basis. ISP support provided by ISP vendors (see Component: Internet Connection above).
Wireless data network for mobile computing network	The City provides a wireless mobile computing infrastructure using LTE cellular technology. Access to the City network is provided via a leased circuit (backhaul) for Seattle Fire Department and via the City internet connection for other departments	Wireless support is provided by Verizon Wireless. Backhaul circuit support is provided by Verizon. City data network connectivity support is provided by ITD Network Engineering & Operations. ISP support provided by ISP vendors (see Component: Internet Connection above).
Cellular telephones	The City provides cellular service to over 2,000 users. Multiple service providers have been engaged by the City which include: AT&T, and Verizon. City is currently working with T-Mobile to add them as another available service. ITD manages the City vendor relationship with the carriers, managed mobility service and billing; but the departments manage their own service effective 09/30/206.	First level support by various business units. ITD End User Support provides vendor relations and coordination and enterprise level service outages. Second level support by service providers (eg. AT&T, Verizon, T-Mobile)
Text Messaging	Text messaging is available on standard cellular phones and smart phones.	Support provided by ITD End User Device Support and service providers.

City Communications Infrastructure		
Radio - 450 MHz Seattle Fire Department paging system	Seattle Fire Department operates a three site UHF simulcast alphanumeric paging system that provides alerting to belt worn pagers. The same infrastructure also provides back-up alerting to fire stations in the event of a failure of the Locution IP alerting network.	First responder level communications support by ITD Radio & Communications Infrastructure.
Paging (non- Fire)	The City provides access to a general paging service via SPOK Wireless (formerly USA Mobility). This service is for all non-Seattle Fire Department pagers. Pagers are managed via ITD Radio & Communications Infrastructure. Because this network is fully owned and operated by a commercial service provider, city staff are limited to managing paging devices and have no network support responsibility.	First level support provided by ITD Radio & Communications Infrastructure. Infrastructure support provided by SPOK.
Electronic mail	The City currently has over 13,000 active user email accounts.	First level support provided by ITD Enterprise Services.
WebEOC	ITD provides support of the WebEOC servers.	First level support provided by ITD Systems Operations.
Citywide Web	There are many different communication channels used during an emergency. The Citywide Web Team provides 24-hour support for communications at the JIC. This requires a computer with browser and internet connection at the JIC. Additional Citywide Web Team staff support the JIC remotely and need access to a computer and internet connection particularly for a longer term event. Provide Emergency updates to the public via the Alerts.seattle.gov blog, social media, and the Seattle.gov Web site. All communication via these channels is controlled by the JIC Supervisor.	First and second level support for the website supported by ITD Web Team.

7. ADMINISTRATION

7.1 Cost Accounting and Cost Recovery

Departments, organizations or agencies with lead or support role for this ESF will track all costs based on guidance provided by their organization and the Seattle EOC. Reimbursement of costs is not guaranteed and if provided will likely not cover all costs incurred.

7.2 Annex Maintenance

The previous standard of updating the CEMP every five years has changed to updates being done on an ongoing basis. With information constantly changing, coupled with rapid innovations in technology and science, it only makes sense to favor a dynamic approach to planning.

ESF Coordinators will be responsible for updating their annex on an annual basis. Coordinators will also be responsible for ensuring all Primary and Support department and agency personnel are trained at least annually on the information contained within this annex.

Table 5

RECORD OF CHANGES			
DATE	TYPE	CONTACT	SUMMARY
December 2016	Update	V Wills L Meyers	Completed annual update
May 2015	Update	K Neafcy	Completed annual update

8. TERMS AND DEFINITIONS

- Terms and definitions related to this ESF/Annex.

- See Seattle Comprehensive Emergency Management Plan.

This page intentionally left blank.