
NIMS ICS Communications Unit Leader Training Guide

Course Number 4969



FEMA



NATIONAL DISASTER &
EMERGENCY MANAGEMENT
UNIVERSITY

April 2025

Intentionally Left Blank

Table of Contents

Introduction	1
Chapter 1: Communications Unit Leader Overview	2
Learning Objectives	2
Communications Unit Leader Position Task Book.....	2
COML Responsibilities	2
Initial Priorities	3
COML's Relationships with Others.....	4
Leadership and Communication.....	6
Pause and Reflect.....	7
Chapter 2: ICS Structure and the Communications Unit.....	8
Learning Objectives	8
Logistics Section	8
Information and Communications Technology (ICT) Branch.....	8
ICT Branch Director.....	9
Information Technology Service Unit.....	10
Information Technology Service Unit Leader (ITSL).....	10
Cybersecurity Unit	11
Cybersecurity Unit Leader	11
Communications Unit	12
Incident Communications Technician (COMT)	12
Incident Communications Center Manager (INCM)	13
Incident Tactical Dispatcher (INTD)	13
Radio Operator (RADO).....	13
Message Runners	13
Auxiliary Communicator (AUXC).....	13
Technical Specialist (THSP).....	14
Pause and Reflect.....	15
Chapter 3: Initial Response and Assessment.....	16
Learning Objectives	16
COML Go-Kit	16
Gathering Information/Information Sharing	17
Initial Meetings and Briefings	17
Operational Period Planning Cycle Meetings and Briefings	18
Determining Initial Priorities and Needs.....	20
Resource Ordering	21
Assigning and Tracking Equipment.....	21
Pause and Reflect.....	23

Chapter 4: Frequency Usage and Regulations	24
Learning Objectives	24
Terminology and Conventions of Use	24
Frequency Notation	25
Radio Spectrum Basics	25
Public Safety Radio Bands	27
VHF Low Band	27
VHF High Band	27
UHF Band.....	27
700 and 800 MHz	28
Analog vs. Digital.....	29
Analog Radio	29
Digital Radio.....	29
Radio Systems.....	29
Simplex Systems	30
Remote Base Systems.....	31
Repeater Systems.....	32
Voting or Remote Receivers	33
Simulcast Systems.....	34
Trunking.....	35
System Access	36
Radio Frequency (RF) Interference.....	38
Sources of RF Interference.....	38
Resolving RF Interference	39
Radio Equipment Safety Issues	40
Radio Frequency (RF) Exposure	40
Other Safety Issues.....	40
Local Use Agreements and Special Temporary Authorizations	42
Local Use Agreements	42
Special Temporary Authorizations	43
FCC Rules for Interoperability	43
Pause and Reflect.....	44
Chapter 5: Interoperability	45
Learning Objectives	45
Communications Interoperability.....	45
SAFECOM Interoperability Continuum	45
Swap Radios.....	46
Cache Radios	46
Gateways	47
Concentric Coverage.....	47
Overlapping Coverage.....	48
Cross-Connect Deployment	49

Shared Channels.....	49
Shared Systems	50
Standards-Based Shared Systems	51
Radio Programming	51
Pause and Reflect.....	53
Chapter 6: Incident Communications Systems	54
Learning Objectives	54
Overview of Networks	54
Command Network	54
Tactical Networks.....	54
Air-to-Ground Network	55
Air-to-Air Network	55
Support Network	56
Designing Radio Systems.....	56
Radio System Considerations	57
Commercial Services (Wireless, Satellite, and IT).....	57
Cost Considerations.....	57
Developing the Incident Radio Communications Plan	58
Incident Radio Communications Plan (ICS Form 205).....	58
Communications Resource Availability Worksheet (ICS Form 217A).....	59
Disseminating the Plan.....	60
PACE Framework.....	60
Pause and Reflect.....	61
Chapter 7: Coordination with Other Agencies.....	62
Learning Objective	62
Federal Coordination	62
Joint Field Offices (JFOs).....	62
Emergency Support Function (ESF) Annexes	63
FEMA Disaster Emergency Communications (DEC).....	64
FEMA Urban Search and Rescue (USAR) Teams	64
State/Local Coordination	66
State/Local Emergency Management Agencies (EMAs)	66
Emergency Operations Centers (EOCs)	66
State Urban Search and Rescue Teams (SUSARs).....	67
Tactical Interoperable Communications Plans (TICPs).....	67
Statewide Interoperability Coordinator (SWIC).....	68
Local Communications Point of Contact (POC)	68
Pause and Reflect.....	70
Chapter 8: The Incident Communications Center (ICC).....	71
Learning Objectives	71
Establishing the ICC.....	71

ICC Facilities	72
Mobile Communications Centers.....	73
Managing the ICC.....	73
Staffing and Equipment Considerations.....	74
Communications Log (Form 309)	75
Local Dispatch Center	75
Managing Incidents Within an Incident (IWIs).....	75
Determine Supply Needs.....	76
Pause and Reflect.....	77
Chapter 9: Transition and Demobilization	78
Learning Objectives	78
Transition Planning.....	78
Demobilization Considerations	79
Demobilization and Check-Out.....	80
Demobilization Check-Out (ICS Form 221)	80
Incident Personnel Performance Rating (ICS Form 225)	80
Equipment Demobilization	81
Transfer of Accountable Property	81
Demobilization Documentation	82
After-Action Review (AAR)	82
Pause and Reflect.....	83
Chapter 10: Additional COML Resources	84
Learning Objective	84
Communication Assets Survey and Mapping (CASM) Tool	84
Commercial Wireless and Satellite Service Providers.....	85
Wireless Carrier Services.....	85
Satellite Services	85
Information Technology (IT) Providers	85
The Information Technology Disaster Resource Center (ITDRC)	86
Cisco Crisis Response.....	86
National Interagency Fire Center, NIFC National Interagency Incident Communications Division	86
The National Interoperability Field Operations Guide (NIFOG)	87
CISA Public Safety Library App	88
Priority Telecommunications Services (PTS).....	88
Wireless Priority Service (WPS)	89
Government Emergency Telecommunications Service (GETS)	89
Telecommunications Service Priority (TSP).....	90
PTS Dialer App.....	90
Shared Resources (SHARES)	91
U.S. National Guard	91

Civil Support Teams (CST)	91
Homeland Response Force (HRF).....	92
Other Response Groups	92
Auxiliary Communications (AUXCOMM).....	92
Civil Air Patrol (CAP)	92
Military Auxiliary Radio System (MARS).....	93
Salvation Army	93
Team Rubicon	94
Pause and Reflect.....	95
Sample Documents.....	96
Sample Communications Resource Availability Worksheet (ICS Form 217A).....	96
Sample Communications Log (Form 309)	97

Introduction

The Communications Unit Leader (COML) oversees the Communications Unit, the Incident Communications Center (ICC), and all aspects of incident communications. The role of the COML is critical in managing the complex communications needs of modern emergency responses, which require a blend of technical expertise, strategic planning, and strong leadership skills.

In addition to leading the Communications Unit, the COML is responsible for designing radio systems and installing and maintaining radio communications equipment during an incident. The COML may also be responsible for tracking large amounts of accountable property, such as cache radios and other specialized deployable equipment.

It is highly recommended that COML students possess strong technical knowledge and experience with radio systems prior to attending this course. Prior experience as a Communications Technician (COMT) is recommended before advancing to the COML position. Students lacking familiarity with radio systems will find this course extremely challenging, especially during the Facilitated Learning Experience (FLEX).

This training guide is a resource that prepares those taking on the role of COML to conduct their duties and effectively manage the Communications Unit. The training guide is designed to complement the ICS Training Reference Guide, which is heavily relied upon in this course. Students will use this training guide to help support the completion of pre-work for the NIMS ICS Communications Unit Leader Course.

Chapter 1: Communications Unit Leader Overview

The Communications Unit Leader (COML) is the individual in charge of the Communications Unit who oversees all aspects of incident communications and reports to the Logistics Section Chief (LSC) or an Information and Communications Technology (ICT) Branch Director. The role of the COML is critical in managing the complex communications needs of modern emergency responses, which require a blend of technical expertise, strategic planning, and strong leadership skills.

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Identify the PTB tasks a COML is responsible for performing.
- Describe the relationship of the COML with others inside and outside of the ICS structure.
- Identify leadership and communication skills that the COML needs to manage the Communications Unit.

Communications Unit Leader Position Task Book



The NQS Position Task Book (PTB) details all the competencies and tasks associated with the COML role. Note: The PTBs assigned by your agency or jurisdiction may vary slightly. Search the [Resource Typing Library Tool](https://rtlt.preptoolkit.fema.gov/Public) for your position's PTB. (<https://rtlt.preptoolkit.fema.gov/Public>)

COML Responsibilities

The COML has several key responsibilities within the Incident Command System (ICS) to ensure effective and efficient communications during an incident or event, including:

1. **Developing the communications plan.** The COML is responsible for creating a comprehensive communications plan for the incident or event, including the allocation of frequencies, the deployment of communications equipment, and the establishment of communications networks among incident personnel and external agencies.
2. **Managing communications equipment.** This includes overseeing the inventory, distribution, maintenance, and return of communications devices and systems. The COML ensures that all equipment is operational and that personnel have the necessary devices to communicate effectively.
3. **Managing personnel.** The COML is responsible for supervising and managing incident personnel assigned to the Communications Unit and Incident Communications Center (ICC).

4. **Establishing the Incident Communications Center (ICC).** The COML sets up and manages the ICC, as needed, which serves as the hub for all incident-related communications. This involves coordinating the flow of information within the incident command structure and with external partners. However, an ICC is not required for all incidents.
5. **Ensuring interoperability.** A crucial responsibility of the COML is to ensure interoperable communications systems are available where they are needed. This often involves coordinating frequencies, integrating different communications technologies, and solving any compatibility issues.
6. **Providing technical support and troubleshooting.** The COML provides technical expertise to resolve issues with communications systems and equipment. This includes troubleshooting problems and ensuring communications lines remain operational throughout the incident.
7. **Monitoring communications.** The COML monitors communications pathways to ensure reliable communications systems are available throughout the incident. This also involves adjusting the communications plan to meet changing needs as the incident evolves.
8. **Providing training and guidance.** The COML offers “just in time” training and guidance to incident personnel on the proper use of communications equipment and protocols as necessary. This ensures that everyone understands how to communicate effectively and securely.
9. **Coordinating with external agencies.** The COML coordinates communications efforts with external agencies, including state, local, tribal, territorial, and federal entities, non-governmental organizations (NGOs), and private sector partners. This is essential for ensuring a unified response and maintaining situational awareness.
10. **Documenting and record-keeping.** Keeping detailed records of communications plans, equipment inventories, and communications logs is another important responsibility of the COML. This documentation is crucial for accountability, post-incident analysis, and planning for future incidents.

Initial Priorities

Upon arriving at an incident, the COML will have many priorities that require attention. As the situation develops, the COML must ensure constant communication with the local communications point of contact (POC), especially if the COML is unfamiliar with the area.

The COML is responsible for ensuring communications pathways throughout the incident, including the various sections of the IMT. The Operations Section usually takes priority; their needs will most likely be handled as the Incident Radio Communications Plan (ICS Form 205) is being constructed. However, incident needs may dictate other priorities. When faced with concurrent priorities, the COML should solicit help setting the priority list from the Logistics Section Chief (LSC) (or the ICT Branch Director if the ICT Branch is established) or the Incident Commander/Unified Command (IC/UC).

Incident priorities may not follow traditional paths. If the operational radio networks are sufficient, other items may take higher priority (e.g., telephone banks to facilitate evacuations). In an all-hazards environment, some communications pathways are likely to be established already through normal channels (e.g., local dispatch or established day-to-day operational communications plans. The COML will need to consider if those communications pathways are sufficient for the entirety of the incident or if supplemental or alternate communications pathways will be needed, especially if mutual aid resources from other areas are expected.

COML's Relationships with Others

The COML will likely interact with several members of the IMT throughout an incident. This table outlines many of the relationships and interactions the COML is likely to establish and maintain; however, this list is not absolute.

Position	Relationship
Local Communications Point of Contact (POC)	Local communications POCs can provide knowledge of existing local communications systems and factors affecting communications in the area and offer support to the COML. The POC could be the local dispatch center, a local or regional Communications Coordinator, an Emergency Support Function (ESF) #2 lead, the Statewide Interoperability Coordinator, or a local system technician.
Incident Commander/ Unified Command (IC/UC)	If the incident does not have an LSC or ICT Branch Director, the COML will work primarily with the Incident Commander/Unified Command to coordinate the placement of equipment and facilities.
Operations Section/Operations Section Chief (OSC)	The COML will work directly with the Operations Section Chief (OSC) to determine how many tactical and support radio nets will be required for the incident or event. A strong working relationship must be established with the Operations Section. The majority of what the COML will need to achieve depends on how Operations chooses to achieve its objectives, how the incident will be functionally or geographically divided, how personnel will be assigned, and what immediate communications needs are required (e.g., life safety and personnel tracking vs. supply orders and tactical direction).

Position	Relationship
Planning Section/Planning Section Chief (PSC)	The COML is responsible for providing documentation of their activities to the Planning Section during the incident. The COML will provide ICS Form 205 for inclusion in the Incident Action Plan (IAP). The COML should review the communications portion of the Assignment List (ICS Form 204) and ensure that the information matches ICS Form 205.
Resources Unit Leader (RESL)	The COML should interact with the RESL to determine what communications resources are assigned, anticipated, or available and to ensure communications resources are allocated efficiently to meet operational needs.
Situation Unit Leader (SITL)	The COML may collaborate with the SITL to illustrate the placement or location of communications assets on maps. From the SITL, the COML may also gain information and situational awareness, such as where the incident may expand, allowing the COML to anticipate future communications needs.
Demobilization Unit Leader (DMOB)	The COML will coordinate with the Demobilization Unit (or designee in the Planning Section if no Demobilization Unit Leader is assigned) to go through the demobilization process using the Demobilization Check-Out (ICS Form 221).
Logistics Section Chief (LSC)	The COML (and the ICT Branch Director, if established) reports to the LSC and will exchange information, provide updates, and plan for the communications-related needs of the incident/event. If any communications equipment is to be demobilized, the COML should identify it and report it to the LSC.
Medical Unit Leader (MEDL)	The COML will meet with the Medical Unit and review the communications aspects of the Medical Plan (ICS Form 206) and other medical-related forms in the IAP to validate/verify any communications requirements listed.
Information and Communications Technology (ICT) Branch Director	If the incident requires significantly expanded communications capabilities, including information technology, cybersecurity, and radio and telephone services, an Information and Communications Technology (ICT) Branch may be established. If this occurs, the COML will report to the ICT Branch Director.

Position	Relationship
Outgoing COML	If there is a transition with another Incident Management Team (IMT) on the incident who has established communications systems and created an Incident Radio Communications Plan (ICS Form 205), the COML for that IMT can provide an overview of the system the team has used, communications equipment that may have been deployed, inventories of any communications equipment on hand, and any challenges experienced at that point.
Incoming COML (if applicable)	If the incident transitions to a new IMT, the current COML will be responsible for providing an overview of the ICS Form 205, current communications systems, communications equipment deployed, inventories of any communications equipment on hand, and any challenges experienced.
Information Technology Service Unit Leader (ITSL)	While the COML primarily deals with traditional communications systems (e.g., radio and phone lines), the ITSL manages digital and IT systems. However, the COML and ITSL roles complement each other by ensuring effective communications and IT support throughout the incident. Often, their duties overlap. For example, they may interact intensively during periods of heightened activity or when specific communications or IT challenges arise that require coordinated troubleshooting and resolution.

Leadership and Communication

Strong leadership, management, and communication skills are essential for COMLs to fulfill their role effectively. The COML is responsible for managing unit personnel and ensuring that team members are well-coordinated. Clear communication is vital for the position and for providing accurate updates to the Logistics Section and other stakeholders. These skills enable the COML to prioritize tasks, guide their team under pressure, foster collaboration, and ensure that tasks are completed efficiently and accurately.



Please refer to the Supervision and Management section of the ICS Training Reference Guide.

Pause and Reflect



Let's take a moment to assess your current skills against the required competencies for the role.

The classroom portion of this training involves group work, so you'll have an opportunity to collaborate with peers to learn and apply your skills.

1. Locate and download the NQS Position Task Book (PTB) for the Communications Unit Leader (COML) position in FEMA's [Resource Typing Library Tool](#).
2. Review the PTB and list the competencies or tasks you want to develop during training. Be ready to share at least one of these areas with the class.
3. What characteristics do you currently possess that would help you to be an effective COML?

Chapter 2: ICS Structure and the Communications Unit

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Identify the purpose, function, structure, and units of the Logistics Section, ICT Branch, and Communications Unit.
- Identify positions within the Communications Unit.
- Identify and differentiate the roles and responsibilities of the COML and the IT Service Unit Leader (ITSL).

Logistics Section



Please refer to the ICS Training Reference Guide and review the functions and responsibilities of the Logistics Section.

Information and Communications Technology (ICT) Branch

The Information and Communications Technology (ICT) Branch is a relatively new addition to the Incident Command System (ICS) structure. It is designed to address the increasing demand for ICT capabilities during incidents. The Logistics Section may use an ICT Branch to manage the span of control and specialized requirements for information and communications technology support during an incident. Depending on the incident needs, the IC/UC may appoint an ICT Branch Director or assign the LSC to manage the COML directly.

The ICT Branch includes personnel with expertise in communications technology and operates under the LSC. The ICT Branch Director oversees ICT operations.

Responsibilities include:

- **Setting up and maintaining infrastructure:** The ICT function is responsible for setting up and maintaining communications and information technology (IT) infrastructure throughout the incident or event.
- **Protection of infrastructure:** The ICT Branch ensures the security and resilience of communications networks, information systems, and technology resources.

- **Coordination and support:** The branch collaborates with other ICS functions and external entities, providing essential support for effective incident management.
- **Adaptation to hazards:** The ICT Branch considers the impact of hazards on ICT capabilities and adapts accordingly to ensure continuity of communications and information flow.

The ICT Branch is composed of:

- The **Communications Unit** is responsible for managing the installation and distribution of communications equipment.
- The **Information Technology (IT) Service Unit** is responsible for technology infrastructure.
- The **Cybersecurity Unit** is responsible for maintaining secure ICT operations.

The ICS organizational structure can be scaled to incorporate additional elements based on the type, size, scope, and complexity of an incident or planned event. The ICS organizational structure builds from the top downward, starting with incident command. If one individual can manage each functional area, no additional organization is needed. If a function requires independent management, an individual is assigned to oversee that function. The IC/UC only fills the positions required to support the incident objectives.

The establishment of the ICT Branch does not preclude collaboration among elements within the ICS organization performing communications, IT services, or cybersecurity-related tasks.

ICT functional requirements and personnel demands expand with more complex incidents. When the functional requirements to manage ICT responsibilities for a large and complex incident are beyond the span of control of a single resource or unit, the responsibilities can be divided and delegated to the Communications Unit, IT Service Unit, and/or Cybersecurity Unit.



For more information on the ICT Branch, refer to the *National Incident Management Systems (NIMS) Information and Communications Technology Functional Guidance*, March 2023, at

https://www.fema.gov/sites/default/files/documents/fema_ict-functional-guidance.pdf.

ICT Branch Director

Based on the needs of the incident, the IC/UC can assign the LSC to manage the ICT function or appoint an ICT Branch Director under the LSC. If an ICT Branch is implemented, the ICT Branch Director's responsibilities include:

- Supervising the operations of the Communications Unit, IT Service Unit, and Cybersecurity Unit.
- Participating in Logistics Section briefings and Planning Meetings.

- Coordinating the activities of ICT Branch units.
- Briefing the LSC on ICT Branch activities.

If an ICT Branch is established, the COML reports to the ICT Branch Director. If there is no ICT Branch, then the COML reports to the LSC. If there is no LSC, the COML will report to the IC/UC.

Information Technology Service Unit

If activated, the IT Service Unit establishes and manages secure data network systems and equipment by:

- Documenting all data network requirements.
- Documenting systems and equipment deployed.
- Developing the Incident IT Plan.
- Identifying disruptions to communications paths or IT resources.
- Supervising and operating the ICT Unified Help Desk.
- Distributing and recovering data network equipment assigned to incident personnel.
- Maintaining and repairing data communications equipment onsite.
- Establishing and monitoring data networks for command, tactical, situational awareness, and support units.
- Coordinating with data owners and responders on data storage, access, and maintenance for the duration of the incident.
- Coordinating passwords and security access as directed for the duration of the incident.

Depending on the size and complexity of the incident, an IT Service Unit may not be activated, in which case, the COML may manage these responsibilities.

Information Technology Service Unit Leader (ITSL)

The Information Technology Service Unit Leader (ITSL) manages information and communications technology resources during incidents. The ITSL operates within the Logistics Section and collaborates with other units to provide essential technological support during incidents. The ITSL's role extends to information management, cybersecurity, and application management for various incident-related functions, including command posts, communications centers, tactical operations centers, and field locations.

The ITSL manages the personnel and operational aspects of ICT data services during incidents to ensure that the Incident Commander/Unified Command, emergency managers, and incident/event responders have any necessary access to ICT systems. At the direction of the ITSL, the IT Service Unit staff prepare and implement incident information technology plans and incident cybersecurity plans while also managing the establishment of IT communications systems, equipment, and services.

While the COML is primarily responsible for managing communications technologies and systems at an incident site, the ITSL focuses more on information technology resources, managing data services, cybersecurity, and technology infrastructure that support the command and operational functions of the incident.

Though the COML and ITSL have separate roles and responsibilities, they must always coordinate to maintain system capabilities and performance. This coordination has become increasingly important as data services on incidents have become more prevalent. Additionally, as technologies continue to emerge and evolve, many pieces of equipment may contain both traditional land mobile radio and IT components.

If the IT Service Unit is not activated, these responsibilities may be assigned to the COML.

Cybersecurity Unit

If activated, the Cybersecurity Unit is responsible for identifying cybersecurity vulnerabilities, assessing threats to the ICT infrastructure and the incident management organization, and recommending risk mitigation actions by:

- Planning and managing the technical and operational aspects of meeting the cybersecurity needs of an incident or event.
- Developing and publishing a basic cybersecurity plan.
- Assessing planning needs and collaborating with stakeholders to develop and draft cybersecurity-related policies, plans, practices, and guidelines for implementation.
- Developing strategies and plans for mitigating identified vulnerabilities and threats.
- Preventing and detecting cybersecurity threats.
- Coordinating the development, promotion, and sharing of cybersecurity information both within and outside the ICT Branch and responding organizations.
- Coordinating documentation and ensuring sensitive security information is properly controlled.
- Performing system administration on specialized cyber defense applications and systems or virtual devices.
- Assisting in identifying, prioritizing, and implementing technical infrastructure and key resources utilized in cyber defense efforts.

Cybersecurity Unit Leader

The responsibilities of the Cybersecurity Unit Leader include:

- Planning and managing technical and operational concerns related to the cybersecurity needs of an incident or event.
- Supervising unit personnel.
- Performing the duties of subordinate positions that are not filled or delegated.
- Participating in incident action planning meetings.

- Developing and publishing a basic cybersecurity plan.
- Establishing and supporting on-scene cyber defense and application capabilities.
- Coordinating support with the cybersecurity departments of all responding agencies.
- Ordering or requesting personnel, supplies, and equipment.
- Documenting and escalating incidents that may harm the environment.

Communications Unit

The Communications Unit is a key component of the Logistics Section. Depending on the size and complexity of the incident, the unit may report directly to the LSC or operate as part of the ICT Branch. The Communications Unit is responsible for developing plans for the effective use of incident communications equipment and facilities, installing and testing communications equipment, and managing the distribution of communications equipment to incident personnel.

Other responsibilities include:

- Documenting all radio channel resource assignments.
- Assigning voice radio channels.
- Producing the Incident Radio Communications Plan (ICS Form 205) for all incidents, including both primary and backup talkpaths as needed.
- Establishing voice networks for command, tactical, support, and air units as needed.
- Setting up on-scene telephony.
- Providing any necessary off-incident communications links.
- Installing and testing communications equipment.
- Supervising and operating the ICC.
- Maintaining and repairing communications equipment on-site.
- Maintaining coordination with ICT service providers.

Note: Some areas of responsibility may overlap with those of the IT Service Unit. If the IT Service Unit is activated, the COML should coordinate activities with the ICT Branch Director or IT Service Unit Leader.

Incident Communications Technician (COMT)

The Incident Communications Technician (COMT) works closely with the COML to provide guidance and support in developing the communications plan. The COMT is responsible for:

- Setting up and maintaining communications equipment, coordinating with other personnel, and ensuring effective communication during incidents.
- Assessing radio system coverage requirements or capabilities.

- Installing, testing, and troubleshooting communications equipment and systems.
- Programming (or verifying the programming) of radio equipment.
- Maintaining and repairing equipment.
- Managing cache equipment, batteries, and gateways.
- Distributing and tracking equipment.
- Resolving interference issues.
- Training users on equipment.

Incident Communications Center Manager (INCM)

The Incident Communications Center Manager (INCM) manages the administrative documentation and inventory of the Communications Unit and may be assigned to manage the ICC itself. The INCM also serves as a Radio Operator (RADO) when needed. The INCM supervises Radio Operators (RADOs), Incident Tactical Dispatchers (INTDs), and Auxiliary Communicators (AUXCs) assigned to the ICC and reports to the COML.

Incident Tactical Dispatcher (INTD)

Incident Tactical Dispatchers (INTDs) manage radio traffic, telephone call processing, data communications, and various forms of documentation tasks in the ICC. An INTD can support the ICC as a single resource or as part of an incident tactical dispatch team. INTDs have a much more capable skill set than RADOs. They typically have state-recognized certification, training in Emergency Medical Dispatch, access to secure information systems (e.g., CJIS and NLETS), training in response plans, and the authority to make decisions.

Radio Operator (RADO)

A RADO works under the supervision of the INCM or COML. RADOs staff the ICC using radios and telephones to receive information, document relevant radio and phone traffic, and relay messages between incident personnel.

Message Runners

Message runners assist in the day-to-day operations of a business or organization. They deliver messages, documents, and packages, run errands, and perform basic office duties. Message runners may be required to physically relay messages to areas without communications systems.

Auxiliary Communicator (AUXC)

An Auxiliary Communicator (AUXC) is typically a volunteer position filled by individuals with expertise in amateur radio communications. These individuals are tasked with providing

auxiliary communications support to emergency response agencies, especially when regular communications systems are disrupted, overloaded, or otherwise unavailable.

Auxiliary Communicators (AUXCs) are often affiliated with organizations such as the Amateur Radio Emergency Service ®, Radio Amateur Civil Emergency Service (RACES), or similar groups that work in coordination with governmental agencies during emergencies.

Responsibilities may include:

- Installing approved auxiliary communications equipment per discussion with the COML or INCM.
- Testing all components of auxiliary communications equipment to ensure systems are operational.
- Operating auxiliary communications equipment for voice and data communications.
- Establishing auxiliary communications area(s) of operation.
- Interacting and coordinating with appropriate auxiliary communications operational personnel.

Similarly, “Auxiliary Communications” (AUXCOMM) is an all-inclusive term used by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Wildfire Coordinating Group (NWCG) to describe organizations and personnel that provide various types of communications support to emergency management, public safety, and other government agencies. This includes, but is not limited to, amateur radio, military radio, and citizens band radio (CB).

Technical Specialist (THSP)

In the all-hazards community, “technical specialist” (THSP) is a catch-all term for specialists and technicians providing expertise in a specific area. Examples specific to the Communications Unit may include gateway specialists, cache management specialists, and telephony specialists. Technical specialists may appear in other areas of the ICS structure as well, depending on their specific area of expertise.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. The ICT Branch is a recent addition to the traditional ICS structure. What is its purpose, and why was it added? Have you been deployed in an incident where the ICT Branch was in place? If so, what aspect of the ICT Branch stood out to you and why?
2. How are the responsibilities of the COML and ITSL similar? How do they differ? How might the COML and ITSL handle overlapping areas of responsibility?
3. Have you been a member of a Communications Unit previously? What position? How will this knowledge and experience help you in the COML role? What positions would you like to learn more about and why?

Chapter 3: Initial Response and Assessment

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Identify materials and information that the COML should gather prior to arriving at the incident.
- Relate COML activities and responsibilities to the Operational Period Planning Cycle.

COML Go-Kit

When developing a go-kit, a COML will develop one kit of personal sustainment gear and a second kit of technical equipment needed to perform their job duties. The personal kit should contain a sufficient quantity of supplies to self-sustain for at least 72 hours and other basic items outlined in the ICS Training Reference Guide. Also, when preparing a personal go-kit, the COML should consider the environment in which they are being deployed (i.e., season, temperature, weather, terrain) and be prepared to adjust accordingly.

A COML's technical equipment kit may vary based on the anticipated needs of the incident but may include:

- Handheld global positioning system (GPS)
- Radio programming equipment (e.g., cloning cable, computer), adapters, and suitable tools
- Resource Status Cards (ICS Form 219) for equipment and T-Card racks (unless this is part of IMT equipment)
- Personal protective equipment (PPE)
- Appropriate ICS forms (e.g., ICS Form 205, ICS Form 214)
- Current Tactical Interoperable Communications Plan (TICP), if available
- Inventories or other lists of local and regional communications response equipment
- Preplanned local system coverage maps
- Contact, capability, and availability information for local and regional Communications Technicians and Communications Specialists
- National Interoperability Field Operations Guide (NIFOG)
- State or local field operations guide or policies and procedures, if available

Additionally, a COML will need to consider the amount of equipment they can reasonably take. In certain cases, they may be able to take large caches of equipment in trailers or mobile communications vehicles. However, there are times when a COML will need to make decisions regarding the equipment they can bring based on space or weight limitations for their designated mode of travel.

Gathering Information/Information Sharing

During the initial activation phase, a COML will likely gather information before arriving at the incident scene. This may include researching the local radio environment using publicly available resources, speaking with other COMLs in the region or state, and monitoring scanner traffic to maintain situational awareness (either through the Land Mobile Radio system or an internet-based hosting service).

As a COML, you may also need to share this information with incoming responders and other communications professionals. Keeping a prepared Communications Resource Availability Worksheet (ICS Form 217A) with local frequencies can be valuable for determining appropriate communications paths. Additionally, you might be asked to provide a list of deployable cache equipment or information about local communications systems.

The amount and types of information shared depend on incident needs but may be influenced by the level of trust between the COML and other parties. Building relationships with other COMLs in your area, state, and region is crucial for effective communication. Consider connecting with the local Statewide Interoperability Coordinator in the state where this event is located; they can provide resources if you are deployed outside of your usual area.

Initial Meetings and Briefings

As part of the initial briefing package, the Agency Administrator Briefing or deployment order, communications system details, or contact information should be provided. The COML should actively seek this information by inquiring with the LSC (or ICT Branch Director, if activated) or appropriate Authority Having Jurisdiction (AHJ) representatives.

A COML may search for information such as the current communications environment, any known gaps that need consideration, and anticipated needs for upcoming operational periods. When a COML arrives at an incident, it is crucial to recognize the likelihood of an existing communications system using the normal channels for that area. The COML must evaluate whether the existing communications plan is sustainable not only for current responders but also for incoming responders who may use various equipment on different systems.

Often, the COML will need to consult with multiple sources to build a comprehensive picture of the communications systems. In addition to the Agency Administrator Briefing (which the COML may or may not attend, depending on the incident), the COML should connect with someone familiar with local communications. This could include a communications center or Public Safety Answering Point (PSAP) manager, radio systems administrator, or another local COML.

Note: Because of the amount of information conveyed during these initial meetings and briefings, it may be useful to record the briefing on your phone and take pictures of maps and organizational charts for future reference.

Operational Period Planning Cycle Meetings and Briefings

COML and the Planning P

Although the COML may not have a large role in the meetings in the Planning P, they do play a very important role in the production of the IAP. The COML will require information from the OSC and PSC to complete the Incident Radio Communications Plan (ICS Form 205).

This information can be acquired through direct contact with these personnel or by attending the meetings where the IAP content is developed. Conversely, the COML may have information that is critical to the OSC when deciding which strategies and tactics to use. For example, the COML may know that the communications infrastructure is insufficient to support proposed strategies, making it necessary to consider a different approach.

In general, the more complicated the incident, the greater the likelihood that the COML will be called upon to be part of the larger IAP design process. However, during some larger incidents, it may seem that incident communications become lost in the shuffle.

Although Command and General Staff may request the presence of a COML at any given meeting, the COML should seek to sit in meetings whenever they have something to contribute (e.g., to address communications issues or infrastructure concerns) or when they need information to do their job (e.g., the number of channels or special equipment required, area requiring radio coverage, or operational concerns).

Note: The COML's most significant contribution to the Operational Period Planning Cycle may actually occur prior to and immediately following the Planning Meeting. This is when the COML drafts and then finalizes ICS Form 205.

Strategy Meeting/Command and General Staff Meeting

Whenever possible, the COML should seek to attend the Strategy Meeting/Command and General Staff Meeting. During this meeting, strategies are built to meet the incident objectives set by the IC/UC. Communications play a major role in executing incident objectives. The COML should collect information related to the intended objectives and strategies for the upcoming operational period. This will assist with building a communications plan that anticipates and meets the needs of the IMT and incident responders.

The COML should provide information on potential concerns related to the communications capabilities of responding personnel. If there are radio dead spaces in the field, complications due to the number of agencies bringing non-compatible radios, or issues with communications infrastructure, the COML should provide this information so issues can be considered while objectives are being evaluated and strategies are being developed.

Tactics Meeting

The Tactics Meeting is used to develop and confirm acceptable tactics that fulfill the strategy needs defined previously. Similar to the Strategy Meeting/Command and General Staff Meeting, the COML may or may not be considered a regular participant. However, the COML may have information critical to tactical success and should try to be present during the development of the incident tactics (which occurs before the meeting) and the meeting itself. This will enable the COML to brief on the Communications Unit's ability to meet the communications needs of tactical assets. The COML should also collect information on the tactics used to draft ICS Form 205 and review the communications information used in the supporting Assignment Lists (ICS Form 204).

Planning Meeting

The COML should participate in the Planning Meeting to brief on the draft Incident Radio Communications Plan (ICS Form 205) and may also participate in planning on an ad hoc basis, as needed. For the COML, this meeting also represents the last opportunity to express concerns about whether the existing communications systems and plans can support the objectives, strategies, and tactics. However, whenever possible, these concerns should be expressed well before the Planning Meeting.

Communicating with Supervisor

At various times throughout an incident, it will be necessary for the COML to have informal briefings or discussions with their designated supervisor to update them on the activities within the Communications Unit, as well as any challenges that may be present. Depending on the scope of the incident, the COML's supervisor is likely to be either the LSC or the ICT Branch Director. These discussions may take place at any time during the planning cycle.

It is important to note that your supervisor may not have a strong communications background, particularly in the all-hazards environment. It may be necessary to tailor the briefing to ensure that your supervisor fully understands what you are trying to convey. Use plain language and avoid technical jargon during the briefing.

Some topics may include:

- Communication Unit needs
- Current radio frequencies and systems in use
- Issues with local communications systems

During these briefings, the supervisor may also provide information to the COML, such as:

- An overview of what is happening at the incident and the significance of those occurrences.
- The appropriate documentation, including the Incident Briefing (ICS Form 201), the IAP, and any additional information deemed relevant.
- The overall goal/mission of the incident response team, as well as the method, means, and schedule the team plans to employ.
- Frequencies that have been allocated, equipment that has already been deployed, and projections for future communications needs.

Communications Unit Briefing

As a COML, you may supervise a group of personnel within the Communications Unit. It is crucial that all unit members are briefed and kept up to date on relevant issues. You should brief the unit often, particularly in the following situations:

- At the beginning of an operational period.
- When new personnel join the unit.
- When significant changes have occurred.
- At the end of each operational period.

These briefings should include a review of the IAP, including ICS Forms 204, 205, and 206, if available. If no IAP is available, review ICS Form 201, which covers:

- Assigned frequencies and talkgroups
- Current and ordered resources
- Incident maps
- Weather conditions
- Medical emergencies
- Current equipment locations

Determining Initial Priorities and Needs

Upon arrival, the COML should conduct a needs assessment. That may happen formally or informally, depending on the incident. The COML should take into consideration the information they have available, including any discussions that they have with other IMT members, to prioritize needs based on:

- The potential threat to life and safety if communications are not established.
- The urgency of the need vs. the availability of necessary resources to establish communications.
- Feasible options for establishing communications.

Resource Ordering

Resource ordering is based on a dynamic, constantly changing incident environment; the COML should continually re-evaluate their resource needs.

- The COML will follow the established process for ordering resources for the incident.
- Communications equipment can be highly specialized. It may be necessary to work closely with the Logistics Section when placing orders.
- If substitutions are required for requested items, the COML should understand what alternatives are acceptable. Sometimes, alternatives may offer only partial functionality or present limitations based on factors such as accessories or programming capabilities.
- If a COML can provide a source for the resources they want to order, it can help ensure they receive the correct resources.

During an incident, there is potentially more than one approach to requesting or ordering resources. It is important to know and understand the ordering forms or systems that your organization uses. If you are sent by your state agency, how do you request support? Are you reliant on local ordering systems? These are vital questions that should be discussed prior to arrival or as soon as possible after receiving the Initial Briefing from the Agency Administrator or IC/UC.

Utilizing the General Message (ICS Form 213), Resource Request Message (ICS Form 213RR), or a similar form or system is recommended for properly managing resource orders.

Note: Be cognizant of any financial restrictions, delivery timelines, or availability issues that may affect resource ordering.

Assigning and Tracking Equipment

A COML is frequently responsible for expensive equipment. Having an adequate tracking system is crucial. This equipment can include more than just radios; it can also include other items such as:

- Portable repeaters
- Laptops/tablets
- Cellular gateways
- Automatic vehicle location (AVL) tracking devices
- Other IT equipment

The systems a COML can use to track equipment can take various forms, such as:

- Pre-printed sign-out sheets
- Resource Status Cards (ICS Form 219)

- Hand receipts
- Electronic tracking

Be sure to account for all components of the equipment you are tracking. For example, if a radio was issued with accessories such as a lapel microphone and extra batteries, make certain that all of the accessories are documented and returned.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. Take a moment to write down a list of the key items you currently have in your go-kit.
2. Based on your reading and review, can you think of any other items you should add to your go-kit as a COML?
3. What information can you obtain prior to arriving at the incident?
4. Where (and from whom) can you gather information upon arrival? What questions would you have?
5. How would you go about determining initial incident priorities and needs?

Chapter 4: Frequency Usage and Regulations

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Identify the public safety spectrum bands.
- Identify common types of radio systems.
- Identify radio frequency (RF) safety issues.
- Describe Local Use Agreements (LUAs) and Special Temporary Authorizations (STAs).

Terminology and Conventions of Use

To develop the Incident Radio Communications Plan (ICS Form 205), the COML must recognize the differences between frequencies, channels, and talkgroups. The COML must also know how to properly record frequencies on incident forms.

- **Frequency.** In the context of radio communications, a frequency is a specific point within the radio spectrum designated for transmitting voice or data signals. Much like a physical address identifies a specific location, a frequency pinpoints a particular segment of the electromagnetic spectrum that can be used for communications. Frequencies are measured in hertz (Hz), megahertz (MHz), or gigahertz (GHz) and serve as the fundamental building blocks of wireless communications, allowing for the transmission of information over distances without the need for physical connections. A single frequency is used for simplex communications. In repeater operations, a pair of frequencies is used: one for transmit and another for receive.
- **Channel.** A channel is a setting on the radio. It is a set of parameters that includes a frequency, a pair of frequencies, or talkgroup information allocated for a specific communications purpose. It is the pathway through which voice or data is transmitted from one point to another. Channels are pre-set into radio devices to facilitate easy access by using a knob or keypad. Channel parameters may also include Continuous Tone-Coded Squelch System (CTCSS) tones, Digital Coded Squelch (DCS) codes, P25 Network Access Codes (NACs), talkgroup IDs, and encryption settings.
- **Talkgroup.** In advanced radio systems, particularly those using trunking technology, a talkgroup operates as a “virtual” channel that enables group communication. To the user, a talkgroup may appear identical to a channel, but behind the scenes, the radio is constantly seeking and acquiring different frequencies as needed to provide a reliable “talkpath” for the user. Unlike traditional channels that are tied to specific frequencies, talkgroups operate within a trunked radio system that dynamically allocates frequencies from a shared pool. This allows for efficient use of the

spectrum, as frequencies are assigned to active talkgroups as needed rather than being permanently dedicated to specific channels.

Frequency Notation

When denoting radio frequencies, accuracy and clarity are essential. Land mobile radio frequencies are referenced in millions of hertz or megahertz (MHz). Radio frequencies should be written out to the fifth digit after the decimal point on ICS forms. This practice is crucial for several reasons. It ensures that radio equipment is programmed with precision, eliminating any room for error that might arise from less precise notations.

Bandwidth refers to the range of frequencies over which a radio signal is transmitted or received. It is defined as the difference between the highest and the lowest frequency of a particular type of electromagnetic wave signal. Bandwidth is a key concept in telecommunications, including radio communications, because it affects the amount of data or information that can be carried over a particular channel.

“Narrowband” signals are typically 12.5 kHz, and “wideband” signals are typically 25 kHz. Wider bands can carry more information and support higher data rates, making them suitable for applications like high-speed data services. However, they are more prone to noise and interference because they cover a wider spectrum. Narrow bandwidths, on the other hand, cannot carry as much data but require less power and can be transmitted over longer distances.

When completing the Incident Radio Communications Plan (ICS Form 205), you must denote receive (RX) and transmit (TX) frequencies with “N” for narrowband or “W” for wideband.

Example: 155.47500 N

Note: Frequencies for trunked systems are not recorded on ICS forms.

Radio Spectrum Basics

Radio spectrum refers to concepts and principles related to the allocation, propagation, and usage of electromagnetic frequencies. Radio spectrum is essential for designing, deploying, and managing communications systems effectively. Here is an overview of the key aspects:

- **Electromagnetic Spectrum.** The electromagnetic spectrum is the full range of electromagnetic radiation organized by frequency or wavelength. The spectrum is divided into separate bands, with different names for the electromagnetic waves within each band. From low to high frequency, these are radio waves, microwaves, infrared, visible light, ultraviolet, X-rays, and gamma rays.
- **Radio Spectrum.** The radio spectrum is a portion of the electromagnetic spectrum with frequencies from 3 Hz to 3,000 GHz (3 THz). This is broken into large swaths

based on certain characteristics of how the spectrum behaves. Some of these include High Frequency (HF), Very High Frequency (VHF), and Ultra High Frequency (UHF). Each part is allocated for specific communications services and applications. Common public safety frequency bands include:

- **VHF low band** – 30-50 MHz
- **VHF high band** – 136-174 MHz
- **UHF** – 380-470 MHz
- **UHF T-band** – 470-512 MHz (not available in all areas)
- **700/800** – 769-896 MHz

These main bands are broken into smaller sub-bands and assigned for specific uses.

- **Radio Wave Propagation.** Refers to how radio waves behave as they travel and interact with various environmental factors. Factors such as frequency, antenna height, terrain, and atmospheric conditions influence propagation characteristics, including range, coverage, and susceptibility to interference. A general rule of thumb is that the lower the frequency, the more easily the signal will travel over terrain, and the higher the frequency, the more line-of-sight it becomes. As frequency increases, a stronger signal will be required to cover the same distance. However, higher frequencies will more readily penetrate into buildings and other structures.
- **Regulatory Framework.** In the United States, radio spectrum is allocated (and its usage regulated) by the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). The FCC regulates private, commercial, state, local, and tribal government allocations. The NTIA, within the Department of Commerce, regulates federal allocations, including those of the military. Some portions of the spectrum are jointly managed.
- **Frequency Allocation.** Refers to the process of designating specific frequency bands within the radio spectrum for particular uses or services. This is done to ensure that different types of radio communications can operate without interfering with each other. For example, certain frequency bands are allocated for services such as broadcasting, aviation, maritime, public safety, mobile communications, and amateur radio. The allocation is managed by national and international regulatory bodies, such as the FCC in the United States and the International Telecommunication Union (ITU) globally.

Note: In radio communications, “line-of-sight” (LoS) refers to a direct path between the transmitting and receiving antennas without any obstructions in between. This means that the radio waves travel in a straight line from the source to the receiver, similar to how light travels.

Public Safety Radio Bands

VHF Low Band

This is the lowest frequency band used in typical public safety operations and occupies the 30-50 MHz spectrum. This band performs very well in mountainous terrain, primarily because the radio waves conform to the terrain. However, it is highly susceptible to long-distance “skip,” solar interference, and sources of noise like electric motors, transformers, and high-voltage power lines. There is no correlation between transmit and receive frequency on repeater pairs — the splits are random. Operation on this band is primarily analog. There is very little digital equipment available.

VHF High Band

VHF high band is widely mixed-use but is one of the most commonly used public safety bands. It has several sub-bands:

- **108-137 MHz** – Exclusive to aviation (AM modulation)
- **138-144 MHz** – Exclusive to federal (primarily military)
- **144-148 MHz** – Amateur radio
- **148-150 MHz** – Shared mobile and satellite
- **150-162 MHz** – State and local, public and private
- **156-157, 161-162 MHz** – Marine band
- **162-174 MHz** – Primarily federal

This band provides good medium-range propagation as the signal will bend somewhat to follow terrain but is more line-of-sight than Low Band VHF. There is no correlation between transmit and receive frequency on repeater pairs — the splits are random. Operation on this band can be analog, digital, or mixed on the same system.

UHF Band

The UHF Band is also widely mixed-use. It is used heavily by both public safety and business/industrial users. It has several sub-bands:

- **406-420 MHz** – Federal use
- **420-450 MHz** – Amateur radio and federal radiolocation
- **450-470 MHz** – Non-federal public and industrial/business

- **470-512 MHz** – Non-federal public safety and industrial/business — this is called the UHF T-band. It is only available in 14 major metropolitan areas and uses the spectrum that was allocated for TV channels 14-20.

This band is much more line-of-sight than VHF bands. It can also be more affected by wet leaves on trees and other vegetation. However, the shorter wavelength offers better penetration of buildings and other structures. This band is more commonly used in medium and large urban areas.

Frequency pairs are standardized in the UHF band. The separation between transmit and receive frequency in a repeater pair is always:

- **9 MHz** in the **380-420 MHz** range
- **5 MHz** in the **420-470 MHz** range
- **3 MHz** in the **470-512 MHz** range

Operation on this band can be analog, digital, or mixed on the same system.

700 and 800 MHz

While still technically part of the UHF spectrum, because of technology limitations, 700 and 800 MHz are separate, unique spectrum segments. For many years, the two bands were separate from each other, but modern radio equipment has made it possible for both bands to operate on the same radio as a single band. While discussed together here, it is important to note that some older radio equipment may not be capable of operating on the 700 MHz portion of the spectrum. These bands are mixed-use and widely used for large trunked radio systems and other digital technologies by both public safety and business/industrial users. The sub-bands are:

- **769-775 / 799-805** – Public Safety
- **806-808 / 851-854** – Radio Communications National Public Safety Planning Advisory Committee (NPSPAC) public safety use
- **809-815 / 854-860** – General pool (business and public safety)

The 700/800 MHz section of the spectrum is even more line-of-sight than VHF and UHF. It can be heavily affected by vegetation like long pine needles and reflects more readily off of hard objects like concrete, rock, and steel. It penetrates structures even better than UHF, as it can enter through windows and other voids in solid building material.

Frequency pairs are standardized — 30 MHz in the 700 MHz range and 45 MHz in the 800 MHz range. Operation in this band varies somewhat. With all but a few exceptions, the 700 MHz spectrum is required to be P25 digital. While much of the usage in the 800 MHz spectrum is digital, there is no requirement that it be a specific format or even digital at all — there are still analog operations in the 800 MHz spectrum.

Analog vs. Digital

Analog Radio

Analog radio systems have been the cornerstone of public safety communications for decades. Known for their simplicity and reliability, analog systems transmit signals that gradually degrade in quality as the distance from the source increases. This degradation, often manifesting as static or noise, becomes more pronounced at the limits of the signal's range. However, this feature also provides users with an intuitive sense of the signal's strength and range, as they can literally "hear" when they are moving out of effective communication range.

Frequency modulation (FM) has been used predominantly with analog radio, but amplitude modulation (AM) is still in use, notably for aircraft.

Digital Radio

Digital radio systems represent a significant evolution in communications technology. Utilizing a digital voice encoder-decoder (vocoder), these systems convert sound into digital signals, which are then transmitted and converted back into sound at the receiving end.

This digital conversion process maintains a consistent audio quality across the coverage area, right up to the point where the signal abruptly cuts off once out of range — there is no gradual degradation as with analog. While this ensures clear communication within the coverage area, it also introduces challenges in high-noise environments where the vocoder might struggle to convert sounds accurately into a digital format. Moreover, digital signals can be compromised by interference from third-party transmitters, potentially leading to dropped communications if the system mistakenly prioritizes the wrong signal.

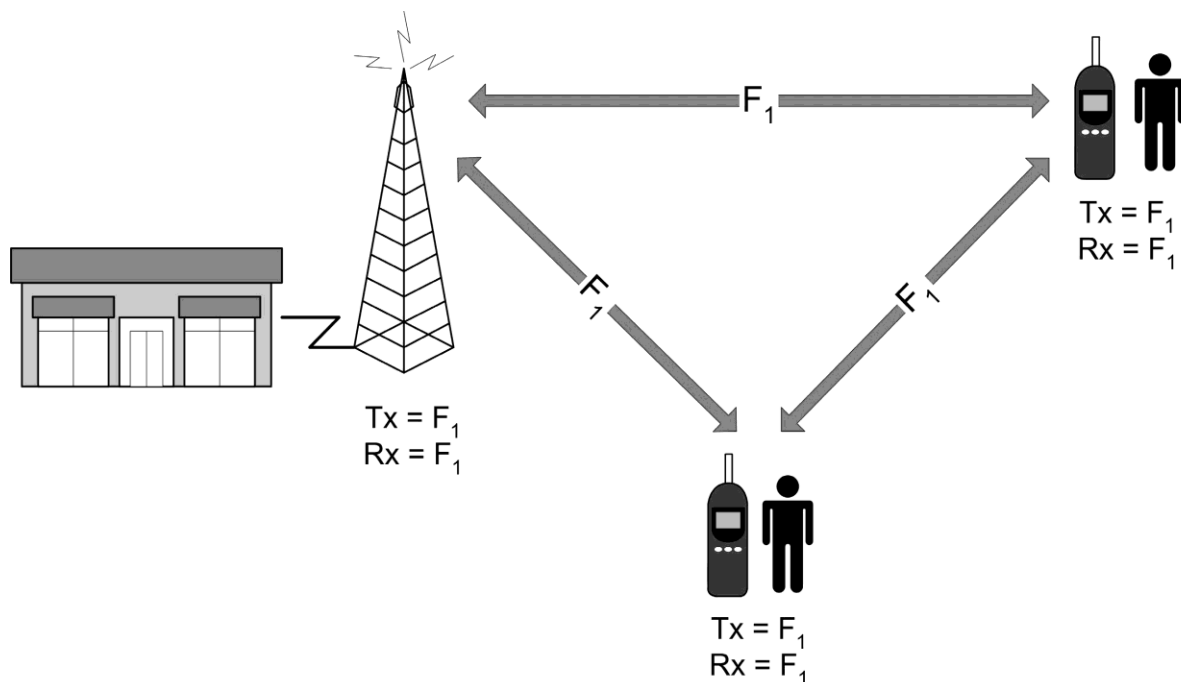
Radio Systems

Conventional radio systems serve as the backbone of incident communications, offering multiple modes to suit different operational requirements. These systems range from basic simplex communications to more sophisticated setups such as simulcast and repeater systems with voting. Each mode has unique features designed to enhance the efficacy and reach of radio communications across diverse environments.

Simplex Systems

Simplex radio systems represent the most straightforward communications mode, functioning on a single frequency for both transmitting and receiving. This mode is renowned for its reliability and simplicity, facilitating direct, line-of-sight communication between units. Ideal for short-range tactical applications, simplex systems are commonly used in scenarios where direct, uncomplicated communications are paramount. Simplex radio is not dependent upon a system and, as such, can still function during a radio system outage.

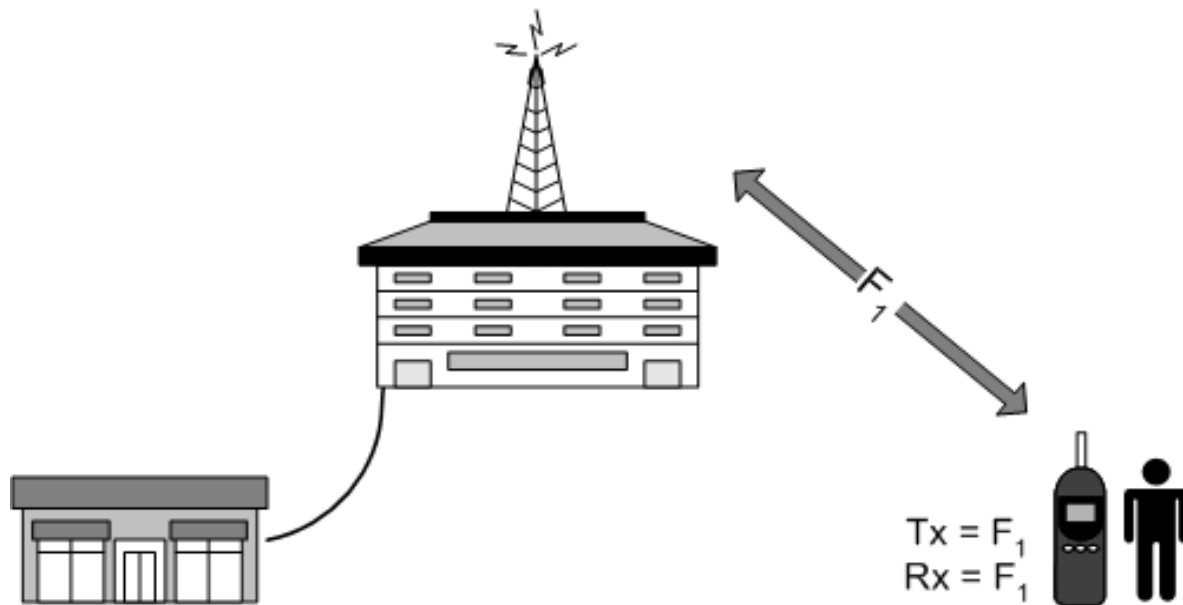
Figure 1. Simplex Radio System



Remote Base Systems

Remote Base Systems extend the utility of simplex by enhancing the base station's range. By strategically positioning the base radio on elevated structures, such as towers or hilltops, the system achieves greater coverage, bridging the distance between the base station and mobile or portable units. This setup significantly improves the reach of base-to-mobile communications.

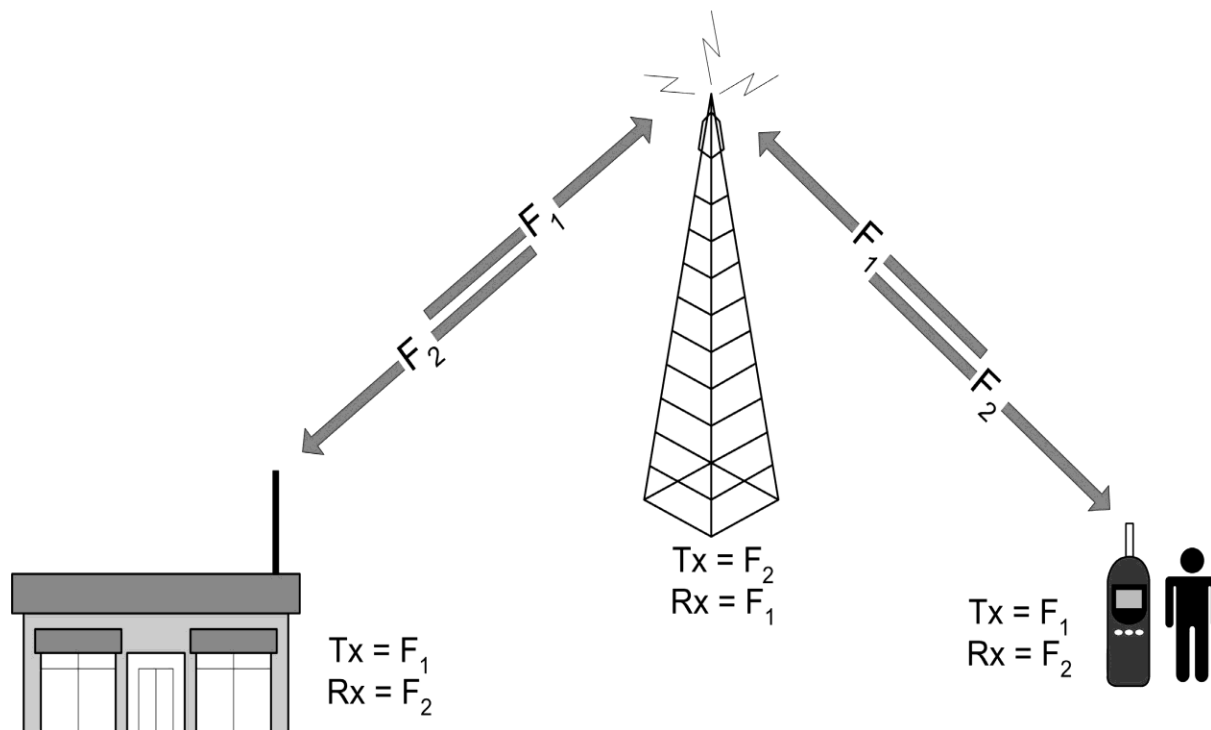
Figure 2. Remote Base System



Repeater Systems

Repeater systems employ two distinct frequencies — one for input and another for output — allowing for real-time retransmission of signals. A repeater is capable of receiving and transmitting at the same time. When it performs this operation, it is described as “duplex.” However, because end-user devices can only receive or transmit (but not both at the same time), the system as a whole is referred to as “half duplex.” This architecture enables communications over vast distances and through challenging terrains by effectively relaying messages from portable and mobile radios through a repeater station. The repeater's elevated or strategic placement ensures widespread coverage, dramatically enhancing the capability of low-power radios to communicate over extensive areas.

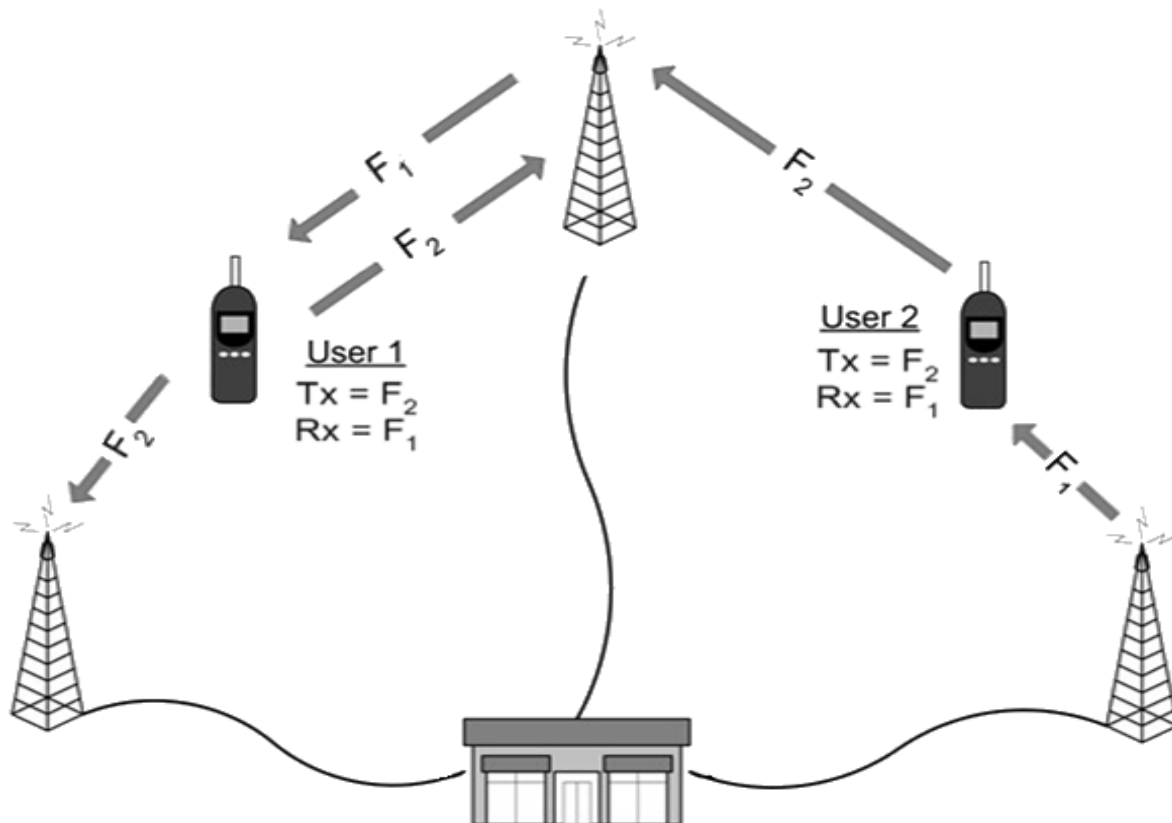
Figure 3. Repeater System



Voting or Remote Receivers

Voting or remote receivers take the repeater concept further by incorporating multiple receivers scattered across various locations. These receivers pick up signals from portable radios, and through a voting mechanism, the system selects the strongest signal to relay. This sophisticated approach balances the system to optimize coverage for portable radios, ensuring reliable communications in environments where direct signals might be hindered by obstacles or terrain.

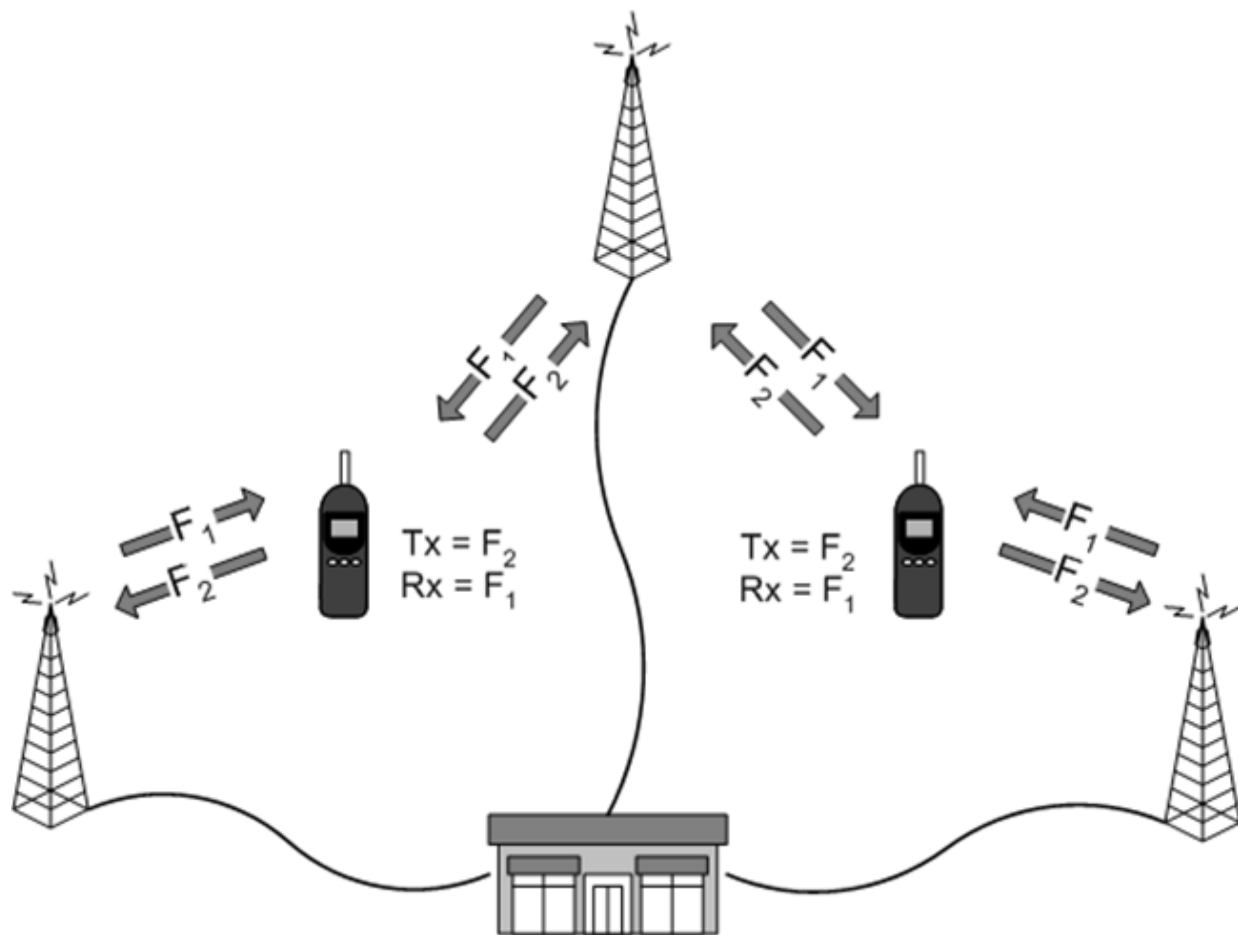
Figure 4. Voting/Remote Receivers



Simulcast Systems

Simulcast Systems offer synchronized transmission of identical signals across multiple transmitters or repeaters, which can significantly improve radio coverage over a large area. Simulcast networks require precise timing, achieved through GPS technology, to broadcast uniform traffic simultaneously over a broad area. This method reduces the likelihood of dead zones or areas with weak signal strength; however, it requires careful management to prevent heterodyne interference and maintain clarity. Heterodyne interference happens when two different radio signals mix together, creating new signals at different frequencies. If these signals arrive at a receiver with slightly different timings or frequencies, they can mix and create interference, making it hard to hear the original message clearly.

Figure 5. Simulcast System



Trunking

Trunking technology is a dynamic and efficient way of managing radio communications channels within a limited frequency spectrum. Unlike traditional radio systems, where each channel is dedicated to a single purpose or group, trunking systems use a shared pool of channels for all users. This approach is grounded in the theory of probability, aiming to maximize the availability of these channels by dynamically allocating them to users as needed.

A trunked radio system is a computer-controlled communications system wherein dedicated frequencies are assigned to individual groups of users. This efficient allocation ensures that multiple individuals or agencies can use the system simultaneously. When a user transmits, the system dynamically selects an open frequency. When the transmission ends, the frequency becomes available for the next user.

The trunking approach significantly improves the capability of a radio system to handle a high volume of traffic over a limited number of channels. It is particularly advantageous in environments where radio communications are critical and frequent, such as among emergency services, allowing for more conversations to occur simultaneously without the need for a proportionally larger number of channels. Moreover, features like priority access and emergency calls are seamlessly integrated, ensuring critical communications are prioritized.

However, trunking systems are not without limitations. During peak times or in highly congested areas, users may experience "busy" signals, indicating that all available channels are in use. Additionally, the technology's reliance on a central controller and sophisticated programming means that trunked systems can be complex to set up and manage. Compatibility issues may also arise between different vendors' systems due to proprietary technologies, further complicating integration efforts.



To learn more about the concept of radio trunking, watch this short video, *How Does Trunking Work?* (7 minutes) at

<https://www.youtube.com/watch?v=6ZUD10Fht2I>

How a Trunked System Differs

In a conventional system, if the system is in use, you must wait until the current user is finished before you can transmit. This can lead to inefficiencies, particularly in systems with heavy traffic, where users may frequently encounter busy signals.

Conversely, a trunked system operates more dynamically. It utilizes a pool of frequencies or channel pairs that are dynamically assigned as needed. When you key your radio in a trunked system, it sends out a signal to the command channel indicating your readiness to transmit. The system then evaluates available resources and assigns the first available

channel pair for your communication. An acknowledgment tone is sent back, usually signified by a double beep, indicating that it is okay to proceed with the transmission.

This dynamic frequency assignment, coupled with the unique ID required for each radio within the trunked system, makes programming these systems complex. These complexities bring additional technical and security vulnerabilities that must be managed.

As such, it is not feasible for a COML to program trunked radios during an incident. This underscores the importance of having pre-programmed cache radios ready for use when common channels are not available.

Trunked System Capacity

The capacity of a trunked radio system is rooted in the distinction between talkgroups and channels within the trunked system. Unlike traditional systems, where each channel is fixed to a specific group or purpose, trunked systems operate on a dynamic allocation of channels, where a pool of available frequencies (or talkpaths) is shared among users.

Talkgroups represent groups of users that communicate with each other over the system, but not every talkgroup communication necessitates a separate channel. Instead, the system allocates channels (or talkpaths) from a shared pool as needed for active communications. This allocation is managed by the system's control channel, which orchestrates the dynamic assignment of talkpaths to different talkgroups based on the current demand.

Therefore, the capacity of a trunked system is not directly determined by the number of talkgroups it supports but *by the number of available talkpaths* — that is, the number of simultaneous conversations the system can handle. Each site within the system has a fixed number of talkpaths, dictating the total volume of simultaneous communications it can support.

The system's capacity can be influenced by various factors, including the physical coverage of transmission towers (which tend to cover a smaller footprint in trunked systems, particularly those operating in the 700/800 MHz bands versus VHF frequency ranges) and the specific talkpath capabilities designed into each tower. Overall, the trunked system's capacity is a balance between the number of available talkpaths and the operational demand placed on the system by its users.

The COML should understand the system architecture to ensure it is not overloaded.

System Access

Controlling who can access a particular communications channel is crucial for maintaining operational security and reducing the likelihood of interference. Tone-coded squelch systems are used in analog communications to secure system access and may take the form of either a Continuous Tone-Coded Squelch System (CTCSS) or a Digital-Coded Squelch

(DCS). Network Access Codes (NAC) serve a similar purpose in digital communications systems.

These systems are designed to manage system access and reduce interference from other users who are not part of the immediate communication group. This ensures clearer communications channels and enhances interoperability among different agencies by allowing them to use shared frequencies or channels without undue interference from outside sources.

Continuous Tone-Coded Squelch System (CTCSS)

CTCSS adds a low-frequency tone to the radio signal. This tone is inaudible to the human ear but is essential for the system's operation. When a receiver is set to a specific tone, it remains silent (squelched) to any signal that does not include that exact tone. This effectively filters out all other transmissions on the same frequency that do not use the designated tone, minimizing the chance of interference from unrelated communications. It is a bit like having a secret knock to enter a room — only those who know the knock (tone) can gain access.

Digital-Coded Squelch (DCS)

DCS is the digital counterpart to CTCSS. Instead of a continuous tone, DCS uses a digital code. This code is transmitted alongside voice communication. Receivers programmed with the matching code will open their squelch and allow the communication to be heard. Like CTCSS, DCS serves to ensure that only transmissions with the correct digital "password" are received, thereby mitigating interference from other users on the same frequency.

Network Access Codes (NAC)

In P25 digital radio systems, the NAC serves as a key to accessing the communications system. It is a form of digital squelch system that identifies transmissions intended for the receiver. The NAC is attached to each digital packet sent over the air. When a radio transmits, it includes a 3-digit code (in hexadecimal format) along with the signal. Receivers monitor for packets that carry the specific NAC to which they are programmed to respond. If the NAC matches, the receiver processes the transmission; if not, the signal is ignored. This technology enhances security by ensuring that only authorized users can access the system and significantly reduces the risk of interference from external or unauthorized transmissions.

Radio Frequency (RF) Interference

One common issue that COMs may face is radio frequency (RF) interference. Interference is defined as “the effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communications system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy.”

RF interference can disrupt communication by introducing unwanted signals that can interfere with the intended transmission. Interference can degrade communications systems, causing signal distortion, dropout, or complete loss of signal. This can result from a wide range of sources, including other electronic devices, competing radio signals, and environmental factors.

Below are types of interference that can affect communications systems:

- **Physical Interference:** This includes obstacles like buildings, terrain, and atmospheric conditions that can obstruct or weaken signals.
- **Electromagnetic Interference (EMI):** This is generated by electronic devices, power lines, or other sources and can disrupt radio signals.
- **Radio Frequency Interference (RFI):** This is interference caused by other radio transmissions operating on the same frequency or nearby frequencies.
- **Man-made Interference:** This can result from intentional or unintentional actions, such as jamming or electrical equipment malfunctions.

Interference is becoming more of a problem every day as more users occupy the finite spectrum available. There are many sources of interference, including other radio users, thousands of wireless devices, and electronic devices that are not radios, such as microwave ovens or computers.

If you experience RF interference, you may need to be a sleuth to find the cause. Use radio technicians, amateur radio operators (who are very good at direction-finding, as they self-police their own frequencies), or the FCC to assist in locating the source of interference.

Sources of RF Interference

How does interference affect radio communications? Here are some examples:

- Radio congestion
- Ambient electronic, commercial, and industrial noise:
 - Computers
 - Industrial systems (e.g., RF gluing, computer controls)
- High power transmitters
- Intermodulation (the mixing of various frequencies producing new signals at different frequencies than intended) due to:

- Direct frequency mixes in transmitters
- Loose or badly soldered connectors
- Nearby metal objects, including rusty bolts, roof flashing, vent pipes, and fences
- Bidirectional amplifiers (BDAs) (designed to enhance RF signal coverage, particularly where signals are weak or obstructed)
- Digital TV over-the-air (OTA) antenna amplifiers (designed to boost the signal strength of a TV antenna)
- Co-channels (multiple transmitters that operate on the same frequency channel)
- Adjacent channels (when signals from nearby frequency channels interfere with each other)

Resolving RF Interference

When trying to resolve RF interference issues, ask for help if you need it. Most legitimate users will try to work to solve interference issues.

Often, the best way to isolate the cause is to listen. If you hear voice traffic, try to identify the location or capture call signs. The licensees of the call signs can be tracked down using the FCC Universal Licensing System database.

Actions that can be taken to eliminate RF interference may be as simple as following recommended practices when installing equipment. In cases of direct interference from an external source, attempt to contact licensees directly. The FCC database may help identify the source. Also, the FCC may be able to assist in identifying dedicated interference sources.

With the exception of licensed trunked systems, the FCC classifies all other frequencies as “shared” without legal recourse to exclusivity.



For more information on RF interference, mitigation, and reporting requirements, refer to the *National Interoperable Field Operations Guide (NIFOG)* at <https://www.cisa.gov/safecom/field-operations-guides>.

For more information on physical interference, please refer to *SAFECOM Infrastructure Obstructions to Radio Propagation* at https://www.cisa.gov/sites/default/files/publications/21_06016_cisa_safecomncswic_infrastructure-obstructions-radio-propagation.pdf.

See also the *SAFECOM Radio Frequency Interference Best Practices Guidebook* at https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf.

Radio Equipment Safety Issues

The COML needs to anticipate a range of potential safety issues related to handling communications systems and equipment. This section outlines some potentially serious safety concerns.

Radio Frequency (RF) Exposure

Radio frequency (RF) exposure can present a health risk for humans. Typically, this is not an issue with the relatively low-power and low-frequency equipment used in public safety.

However, there may be situations, particularly in workplace environments near high-powered RF sources, where the recommended limits for safe exposure of human beings to RF energy could be exceeded. For example, high-power transmitters can cause physical harm to humans, particularly high-power broadcast antennas like those used for AM radio, FM radio, and TV and radar at military and aviation facilities. Directional antennas such as dishes and Yagi antennas produce more focused energy.

Biological effects resulting from exposure to RF energy, including the heating of tissue by RF energy, are often referred to as “thermal effects.” Exposure to very high RF intensities can result in the heating of biological tissue and an increase in body temperature in a similar manner to the process by which microwave ovens cook food.

Tissue damage in humans could occur during exposure to high RF levels because of the body's inability to cope with or dissipate the excessive heat that could be generated. Soft tissue, such as the eyes, is particularly vulnerable to damage from RF exposure.

The best protection from RF exposure is distance. The exposure level drops by 75% or more each time the distance from the transmitter or source is doubled. The COML should ensure that personnel are aware of safe distances and that areas with potentially hazardous RF levels are clearly marked. When in doubt, consult with an engineer to evaluate the situation.



For information on radio frequency safety, please visit the FCC website at <https://www.fcc.gov/general/radio-frequency-safety-0>.

Other Safety Issues

Adverse Weather Conditions

- **Severe weather.** In addition to creating challenging working conditions for personnel, adverse weather, such as rain, snow, or extreme heat, can affect the performance and safety of communications equipment. The COML should ensure that all

equipment is weather-protected and that there are contingency plans for severe weather.

- **Lightning strikes.** Communication towers and antennas are particularly vulnerable to lightning strikes. Proper grounding and lightning protection systems should be in place to minimize risks.

Electrical Hazards

- **Improper grounding.** Communications equipment, especially mobile or temporary systems, must be properly grounded to prevent electrical shocks or fires. The COML should ensure that all equipment is installed correctly and grounding procedures are followed.
- **Electrical generators.** If generators are used to power communications equipment, they must be set up in well-ventilated areas to avoid carbon monoxide poisoning. The COML should ensure that fuel is stored safely and generators are operated according to safety guidelines. Also, it is extremely important that generators are properly grounded when in use.

Environmental Impacts

- **Hazardous materials.** The use and disposal of batteries, fuel, and other materials associated with communications equipment can pose environmental hazards. The COML should have plans in place for the safe disposal of hazardous materials.

Equipment Transportation and Setup

- **Antenna and mast setup.** Erecting antennas and masts can be hazardous, particularly in high winds or on unstable terrain. When setting up an antenna or mast, there should always be someone else watching to ensure safety and to look out for overhead obstructions such as power lines. The COML should ensure that personnel are trained in safe setup procedures and that all equipment is securely anchored.
- **Transporting equipment.** Moving heavy or bulky communications equipment poses risks of injury. Proper lifting techniques and the use of appropriate transportation tools (like dollies or carts) should be employed. The COML should emphasize the importance of using dollies or carts when lifting heavy communications equipment.

Health and Safety

- **Regulatory compliance.** The COML must ensure that all communications operations comply with relevant health and safety regulations, including those from agencies like OSHA (Occupational Safety and Health Administration) and the FCC (Federal Communications Commission).

- **Fatigue and stress.** Extended operations can lead to fatigue and stress among personnel, which can result in mistakes or accidents. The COML should monitor the workload of communications staff and ensure adequate rest periods.

Interference with Other Systems

Communications systems can sometimes interfere with other electronic equipment, including medical devices or air traffic control systems.

Local Use Agreements and Special Temporary Authorizations

Local Use Agreements (LUAs) are formal agreements that facilitate resource sharing among agencies, while Special Temporary Authorizations (STAs) provide temporary authorization for communications facilities during emergency situations. There are also FCC rules and regulations that play a role in ensuring effective communication during emergencies.

Local Use Agreements

LUAs are formal agreements between different entities (such as government agencies, private organizations, or local jurisdictions) that allow them to share communications resources during emergencies or special events. LUAs enable one agency to utilize the radio system of another without the necessity for the former to obtain a separate channel license. These agreements are permissible exclusively within the geographical boundaries of the issued license. The license holder retains the authority to terminate such agreements at any point. It is recommended that these agreements be formalized through written documentation.

It is important to note that these arrangements are not intended to circumvent the standard licensing requirements. Agencies are bound by the conditions of their own FCC license, particularly regarding their designated operational area. Authorization for use cannot extend beyond the license's stipulated terms. While these agreements need to be formalized in writing, they do not have to be unduly complicated. See 47 CFR § 90.421 for clarification.

This framework facilitates enhanced cooperation and interoperability among various agencies, ensuring that communication remains fluid and effective during joint operations or emergencies. By allowing agencies to share resources within the confines of their licensing agreements, this rule plays a critical role in bolstering public safety and emergency response capabilities.

Special Temporary Authorizations

An STA is a mechanism provided by the FCC that allows entities to use specific radio frequencies temporarily under certain conditions. These authorizations are crucial for addressing immediate communications needs that arise from unexpected situations or emergencies or for conducting short-term operations that necessitate the use of frequencies not covered under an entity's current FCC license.

STAs are designed to offer flexibility and rapid response capability in the spectrum management framework, enabling entities to adapt quickly to changing operational needs or to enhance their communications capacity during critical events. They are allowed for emergencies representing a danger to life and property and are typically granted for six months. STAs are not typically used for planned events or exercises.

The process of obtaining an STA is fairly simple, which ensures timely access to necessary frequencies. Requests can generally be made online. However, entities seeking the STA must provide a justification, the proposed installation or area of operations, the specific frequencies requested, and the duration for which the authorization is needed.

Note: Detailed instructions for requesting an STA can be found in the NIFOG.

FCC Rules for Interoperability

The FCC encourages and coordinates the development of a nationwide, seamless communications system for emergency services. FCC rules and regulations provide nationwide interoperability and mutual aid channels.

47 CFR § 90.421

This rule offers significant flexibility, notably by allowing federal agencies to access VFIRE/UTAC frequencies for which they may not have explicit licenses. Unlike typical licensing protocols, the FCC generally does not issue specific licenses for interoperable frequencies. Instead, permission for their use is implicitly granted through a Part 90 public safety license, a provision not typically applicable to federal agencies since they receive their licensing through the National Telecommunications and Information Administration (NTIA).

Note: FCC rules intended to support emergency radio interoperability, as well as a complete list of nationwide interoperability and mutual aid channels, can be found in the NIFOG.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. What are the basic types of radio systems that can be used during an incident response? What are some of the merits and pitfalls of the various types?
2. What is trunking, and how does it differ from conventional radio systems?
3. What parts of the radio spectrum are used for public safety?
4. What are some common causes of radio interference, and what can you do to prevent or resolve it?
5. What are some safety issues you should consider when handling communications systems and equipment?

Chapter 5: Interoperability

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Explain the concept of interoperability.
- Identify technological resources and systems available to support interoperability.

Communications Interoperability

Communications interoperability refers to the capability of public safety services and support providers to communicate with staff from other responding agencies and to exchange voice and/or data communications on demand and in real-time, as authorized.

SAFECOM Interoperability Continuum

The SAFECOM Interoperability Continuum serves as a foundational framework for enhancing emergency communications and ensuring the operability and interoperability of public safety systems. It addresses critical elements for planning and implementing interoperability solutions. These elements include:

- Governance
- Standard operating procedures (SOPs)
- Technology
- Training and exercises
- Usage of interoperable communications

The continuum is used as a tool at the strategic level for interoperability planning. When acting as a COML on an incident, you will be operating at a tactical level. As such, several of the items listed on the continuum are not things that can be changed in the middle of an incident. However, the COML must understand the concepts of interoperability and ways of working towards better interoperability, as you may be called upon to provide input for pre-planning strategic meetings that will impact the technologies you will have available to you in the future.

Within the continuum, the technology lane is where you can make the most impact through the decisions that you make as a COML during an incident. It is important to remember that all the options presented along the continuum are simply different tools that can be utilized on the incident. Each option has advantages and disadvantages. It is the responsibility of the COML to understand their options to make the best choices for the incident.



For more information on the SAFECOM Interoperability Continuum, refer to SAFECOM Interoperability Continuum: A Tool for Improving Emergency Response Communications and Interoperability (June 2021) at https://www.cisa.gov/sites/default/files/2022-12/21_0615_cisa_safecom_interoperability_continuum_brochure_final.pdf.

Swap Radios

The term "swap radios" refers to radios that are exchanged or deployed to temporarily replace or augment existing communications equipment. This could be part of a strategy to ensure interoperability among various responding agencies or to provide immediate communications solutions in the event of equipment failure, lack of compatibility, or when additional communications resources are required.

Swap radios are typically portable handheld radios that allow responders to switch between different radio channels or talkgroups quickly. Swap radios are often compatible with various radio systems (analog, digital, and trunked) used by different agencies. They are particularly useful when responders need to communicate across various functional groups or incident divisions during an emergency.

Cache Radios

Cache radios refer to pre-stored or stockpiled communications equipment that is held in reserve for emergency deployments. These caches are strategically located for quick deployment to incident sites. The use of cache radios is a planned component of emergency management and incident response, ensuring that adequate communications resources can be quickly made available. Many states and local governments often maintain their own cache radios as part of their emergency preparedness and response strategies. At the federal level, there are radio caches and resource pools that can be quickly mobilized and deployed to support state, local, tribal, and territorial (SLTT) authorities.

Note: Refer to the National Interagency Fire Center (NIFC), NIFC National Interagency Incident Communications Division (NIICD) in the Additional COML Resources section of this guide for more information about cache radio resources.

Gateways

A radio gateway is an intermediary device that facilitates communication between different radio systems or networks. Gateways are used to bridge different communications systems, allowing users on incompatible radio systems to communicate with each other. This is particularly useful in scenarios where multiple agencies with different communications equipment need to work together.

There are typically two types of gateways: fixed and mobile.

- **Fixed gateways** are permanently installed and provide a consistent bridge between specific communications systems. Fixed gateways are typically pre-set with specific radios with settings already configured and may be part of a dispatch console setup.
- **Mobile/portable gateways** are portable and can be deployed as needed on specific incidents, events, or exercises. While some of these may be preconfigured with specific radios, they are often reconfigured on an incident. If so, settings will need to be reestablished as changes in the system configuration are made.

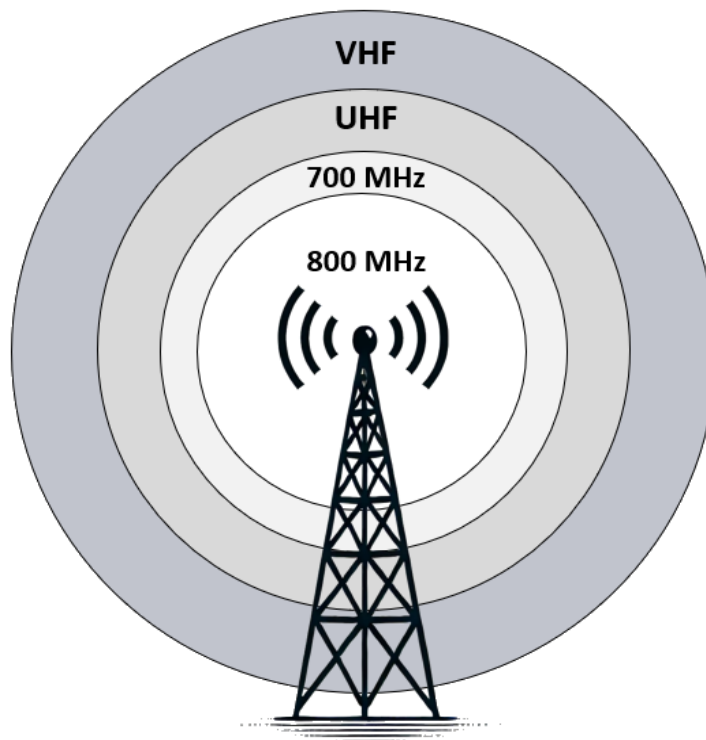
To effectively deploy radio gateways, communications personnel should understand the concepts of **concentric coverage**, **overlapping coverage**, and **cross-connect deployment**.

Together, these concepts highlight strategic considerations necessary for deploying gateways in emergency communications networks. Understanding the coverage areas of different communications systems (concentric coverage), ensuring that these areas overlap (overlapping coverage), and strategically placing gateways in these overlapping areas (cross-connect deployment) are essential steps in achieving interoperable communications during emergencies.

Concentric Coverage

This concept involves understanding the geographical coverage area of different communications bands or systems, which can be visualized as concentric circles around a transmission source. It ensures reliable communications coverage by using multiple overlapping radio coverage areas arranged around a common center. The coverage area tends to decrease as the frequency increases, meaning that lower frequency bands typically offer wider coverage than higher frequency bands. This concept is crucial for planning communications strategies, as it affects how and where communications assets, including gateways, should be deployed.

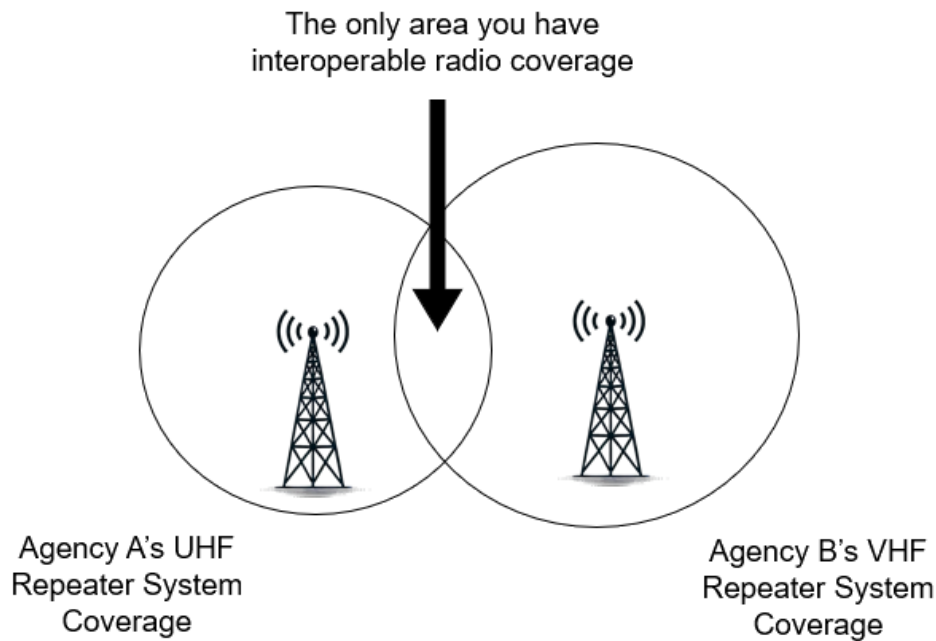
Figure 6. Concentric Coverage



Overlapping Coverage

Overlapping coverage refers to the areas where the coverage zones of two or more communications systems intersect. For gateways to function effectively, they must be deployed within areas of overlapping coverage between the systems they are connecting. This ensures that users on both sides of the gateway can communicate seamlessly across the bridged networks.

Figure 7. Overlapping Coverage



Cross-Connect Deployment

Cross-connect deployment involves placing gateways strategically to bridge communications systems, taking into account concentric and overlapping coverage. By deploying gateways in areas where the coverage of different communications systems overlaps, emergency responders can create a unified communications network that allows for interoperable communications among various agencies and departments. This is particularly important in large-scale incidents where multiple responding agencies with different communications equipment and frequencies must work together efficiently.

Shared Channels

Shared channels support interoperability by providing common frequencies or talkgroups that are established and pre-programmed into radios. This setup allows for interoperable communications between different agencies. The implementation of multi-band portable radios significantly enhances the reality of the shared channel concept across different bands. Interoperability is simplified when agencies share common frequency bands and modulation, whether analog or digital.

This approach to interoperability relies on the simplicity and directness of shared channels as the most straightforward form of interoperability, unlike more complex solutions that might be considered. The selection of shared channels often depends heavily on governance decisions, as long-term choices must be made regarding which organizations

will utilize specific frequencies. Due to general frequency congestion across the United States, there are severe restrictions on the number of independent interoperability talkpaths available in some bands, which also influences the selection and use of shared channels.

Agencies are encouraged to adopt a standard of programming for all the national interoperable channels for their radios, applicable to the radios' capabilities, and to use a standard naming convention to facilitate coordination.

Note: Refer to the National Interoperability Field Operations Guide (NIFOG) for a listing of national interoperable channels.

Shared Systems

Shared systems support interoperability by facilitating the use of a single radio system infrastructure, typically from a single manufacturer, to provide service to several public safety agencies within a region.

By using a single radio system infrastructure, shared systems ensure that all participating agencies can communicate over the same network. This eliminates the compatibility issues that can arise when agencies use different communications systems.

Shared systems are established through considerable coordination and require the selected system to meet the needs of all local organizations involved. This level of planning ensures that interoperability is built into the system from the outset and leverages shared infrastructure to facilitate communication between different agencies without the need for additional interoperability solutions.

With a shared system, cross-connects or gateways become unnecessary for internal communications among participating agencies. Since all components of the system are designed to work together seamlessly, agencies can communicate more easily without the need for additional interfacing equipment.

It is important to note, however, that in the case of trunked radio systems (which are common in shared systems), there are limitations on the number of talk groups or virtual channels that can be effectively accommodated on an incident scene simultaneously. Understanding these limitations is essential for effective communications during large-scale incidents.

Many shared systems are not standards-based and utilize proprietary technology. As such, users are required to purchase radios from a specific manufacturer to ensure compatibility with the infrastructure. The solution to this problem is to utilize a system based on accepted industry standards.

Standards-Based Shared Systems

Standards-based systems support interoperability by promoting the use of common standards across different communications systems, which facilitates seamless communication among various agencies.

Standards-based systems adhere to common protocols defined by recognized standards organizations, such as the Project 25 (P25) standards developed by the Association of Public Safety Communications Officials (APCO). This adherence ensures that communications equipment and systems from different manufacturers are compatible, enabling agencies to communicate across different platforms.

By establishing standards, these systems offer public safety agencies the flexibility to choose from a variety of equipment and system providers. This prevents agencies from being locked into a single vendor's proprietary system, allowing them to select the best equipment to meet their needs while maintaining the ability to communicate with other agencies.

Standards-based systems are designed to be forward-compatible with future developments in communications technology. As standards evolve, equipment can be updated or replaced to remain in compliance with the latest versions, ensuring long-term interoperability and investment protection.

Many standards-based systems include features specifically designed to enhance interoperability, such as mutual aid channels and interoperability talkgroups. These features are built into the system architecture, providing ready-to-use solutions for cross-agency communications during an incident.

Radio Programming

Although it is highly discouraged, it could become necessary to program radios onsite during some incidents or events. These could include cache radios or radios that personnel bring with them. Due to the various brands, models, and versions of radios, it may be challenging to have all of the compatible software, cables, or adapters to program them all.

It is better to explore other solutions first. Should it become necessary, work with local radio technicians to assist in programming. Order cache radios that have been pre-programmed, come with a technical specialist who can program them, or come with the proper software and equipment for programming. These radios can then be issued to incident personnel.

Note: It is essential that the radio system owner is involved any time new radios are added to their system.

Pre-planning of radio programming and establishment of incident response channels/talkgroups can reduce the need for on-scene programming in the majority of situations.

Radio programming involves configuring radio equipment to enable communications on given systems. Before programming begins, the programmer must have all the necessary information to ensure that radios are properly configured to support operations, facilitate coordination among response teams, and maintain connectivity in challenging and dynamic environments.

Caution should be used when programming radios in the field. The transposition of a single digit can render a channel unusable. Pre-programming, verification, and testing are recommended. Also, the cloning of pre-programmed channels is preferred over field programming.

The following are the key duties for radio programming:

- **Channel Configuration.** Program radio channels with specific frequencies, modulation types, and signaling codes to support different teams, functions, and operational areas within the incident command structure.
- **Radio Identification.** Depending on the type of system utilized, radio units may require unique identification codes to facilitate authentication with the system and coordination among personnel and teams. The programmer must ensure each radio unit is correctly labeled and that the ID is registered within the communications system. The programmer must ensure that each radio unit is correctly labeled and that its ID is registered within the communications system.
- **Encryption and Security.** Implement encryption protocols or secure communications modes as needed to protect sensitive information and prevent unauthorized access to communications channels. Ensure that encryption keys or security settings are properly configured and managed to maintain information confidentiality and integrity.
- **Radio Features and Functions.** Configure radio features and functions such as buttons, menus, scanning, and emergency alerts to meet operational requirements.
- **Testing and Validation.** Program a small number of test radios and conduct thorough testing and validation of radio settings and configurations to ensure proper functionality and performance. After verifying proper operation, program all remaining radios.
- **Documentation and Record-Keeping.** Maintain accurate documentation of radio programming settings. Keep detailed records of radio inventory, assignments, and changes to facilitate accountability, troubleshooting, and future reference.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. What is the SAFECOM Interoperability Continuum, and why is it important for incident communications?
2. What are some possible ways that the COML can overcome interoperability issues between responders from different agencies?
3. What are gateways, and how do they work?
4. If you need to deploy a portable gateway, do you know how to access one and how to operate it?

Chapter 6: Incident Communications Systems

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Differentiate between command, tactical, and support networks.
- Identify requirements for establishing an incident radio communications system.
- Identify how to assess communications needs and order resources.

Overview of Networks

The National Incident Management System (NIMS) provides a standardized framework for communications, information management, and information sharing support at all levels of incident management. It ensures that effective, interoperable communications processes, procedures, and systems exist across all agencies and jurisdictions. According to NIMS, the Communications Unit is responsible for ensuring adequate voice and data networks are available. These networks include various communications channels such as command, tactical, air-to-ground, air-to-air, and support networks.

Command Network

The Command and General Staff may use the command network; however, it is more often used as a coordination channel for the Operations Section.

Usually, only one command network is used by the Command and General Staff during an incident. The command network is usually less technically challenging than other networks, given that Command and General Staff tend to remain in the same area around the Incident Command Post (ICP).

The command network may be patched via a gateway when personnel are on disparate radio systems and cache radios can be programmed for its use. For instance, if the OSC is on a system commonly used by firefighters and the PSC is on an emergency medical services (EMS) radio system, cache radios may be used to ensure consistency.

The command network is used as a link between the incident and the dispatch center, enabling communication between the Command and General Staff and other incident networks.

Tactical Networks

Depending on the size of the incident and the command structure, several tactical networks may be needed based on the number of divisions (geographic) and/or groups (functions) required.

Tactical networks could be as simple as designating a common channel to the resources assigned to that division or group. Tactical networks can also be challenging if coverage is required over vast distances, the signal must penetrate objects, or disparate frequency bands are required to be connected within a division or group.

Using common channels is preferred over patching channels of the same frequency band, but patching channels may be required if common channels are not available on all radios or if they cannot be programmed. “Patching” is a generic term that refers to connecting channels, talkgroups, or systems that otherwise cannot communicate with each other.

When patching to a trunked radio system, there is no guarantee that the audio will be transmitted. If the trunked system denies a channel, the patched system (and the person transmitting on that channel) will not know this has occurred.

Air-to-Ground Network

An air-to-ground network is used to coordinate air support during an incident. This can be as simple as designating a common air-to-ground channel to be used between tactical resources and the aircraft.

On larger, complex incidents, multiple air-to-ground channels may be required. A designated “air guard” channel should be established if multiple air-to-ground channels are utilized. This air guard channel would be used only for emergency contact with the aircraft. If an Air Support Group Supervisor or Air Operations Branch Director is established, the COML should coordinate with them when designating air-to-ground and air guard channels.

Care should be used when air assets are using trunked radio systems. If the transmitter is in the air, the signal can interfere with other trunked radio systems or drag traffic to sites where it does not belong, overloading those sites.

Air-to-Air Network

Air-to-air channels are utilized for communication between aircraft. Channels may be designated to communicate with other aircraft on the incident, with aircraft of the same kind, with an Air Tactical Group Supervisor, or with aircraft that may enter the same airspace, such as medical or media aircraft. Ground-based tactical resources should use air-to-ground channels (not air-to-air channels) when communicating with the aircraft.

The Federal Aviation Administration (FAA) does not allocate air-to-air frequencies for people or incident teams to self-assign. The FAA maintains strict control over these frequencies to avoid interference that may cause aircraft safety hazards.

As a result, the COML cannot assign air-to-air frequencies. Instead, they must be ordered from the FAA. An ordering point at a local Emergency Operations Center (EOC) will generally have contact information for the appropriate personnel within the FAA.

If an incident is complex enough to require air-to-air communications, it is recommended that the COML assign someone to staff or utilize a qualified Air Operations Branch Director or an Air Support Group Supervisor familiar with air-to-air technologies and programs.

Support Network

The support (or Logistics) network facilitates coordination between Logistics Section assets. Often, when the Logistics Section is geographically stable, the units within the section may not require many radio systems assets. In such cases, these units require phone, fax, and internet data links.

Based on the nature of the incident, however, the support network could be quite large. Logistics assets could be geographically dispersed, and some elements may also be mobile. Groups on this network may include camps, security, staging, and transportation channels.

Designing Radio Systems

The first step in creating the command network is to perform a needs assessment. This may be done formally or informally, depending on the incident, and may include discussions with others within the ICS structure to determine needs.

When analyzing coverage, the COML may consult local technicians and advisors for input and must also consider:

- **Existing communications systems.** The COML should assess any pre-existing communications systems that might be utilized or incorporated into the incident or event and obtain permission to use them.
- **Terrain and other features.** The COML should consider terrain features and other obstacles that hinder effective communications.
- **Incident objectives.** Understanding the specific goals and objectives of the incident is crucial for designing an effective radio system.
- **Incident size and anticipated growth.** The COML should consider the potential growth of the incident and how it might impact communications needs. This includes scaling the ICS organizational structure and defining operational boundaries.
- **Available equipment.** Assessing the availability of communications equipment is essential. If additional equipment is required, the COML must determine the time needed to acquire, install, and distribute the equipment.
- **Incident coverage needs.** Identifying the areas that require communications coverage is vital. This includes pinpointing Incident Command Post (ICP) and Incident Communications Center (ICC) locations, remote campsites, roads, travel routes, accessibility, and aircraft use (including helibase locations).
- **Staging areas.** The COML should consider communications capabilities in staging areas where resources are deployed.



There are various resources available to analyze the situation, such as FEMA's Geospatial Resource Center at <https://gis-fema.hub.arcgis.com/>.

Radio System Considerations

When designing the command network, the COML must be concerned with several potential problems, such as interference from an adjacent incident or interference with normal daily response radio traffic.

The necessity of establishing multiple repeater sites can also be problematic, as they will prolong the wait for the command network and pose potential interoperability issues.

The COML must also think about what additional equipment may be needed. More complexity means more need for equipment. Repeaters, links, and additional cache radios are required as an incident's communications increase in complexity.

The COML must continually consult with incident leadership and immediately order anything they request, including auxiliary communications services, even if this may pose a burden on the rest of the system.

Commercial Services (Wireless, Satellite, and IT)

Sparse local resources may dictate the need to utilize non-typical alternatives. Utility companies often operate large, robust radio networks. Commercial satellite providers and local telephone and data companies may also offer solutions.

Note: Refer the Additional COML Resources section in this guide for more information on commercial or alternative wireless, satellite, and IT services and support.

Cost Considerations

While it is essential to recognize that the overall financial responsibility for the incident falls to the Finance/Administration Section Chief, all members of the Incident Management Team (IMT) share some responsibility for considering decisions within their purview to prevent duplication, waste, or unnecessary expenses. The COML should provide communications services to the best of their ability while adhering to the budget constraints set by the Finance/Administration Section under the direction of the AHJ.

Often, there are multiple ways to accomplish the same task. In such cases, the COML should weigh expense as one of several factors when determining the most appropriate option for the incident. Other options include:

- Demobilizing unused equipment and canceling temporary services initially set up for the incident to minimize wasteful spending.
- Borrowing cache equipment or arranging temporary leasing options rather than purchasing communications equipment.
- Exploring pre-existing relationships with vendors or communications personnel in the area to identify other viable options.

Developing the Incident Radio Communications Plan

Incident Radio Communications Plan (ICS Form 205)

It is the primary responsibility of the COML to complete the Incident Radio Communications Plan (ICS Form 205), which addresses the radio communications needs of the incident in the most effective manner possible. ICS Form 205 is given to the Planning Section for inclusion in the Incident Action Plan (IAP).

ICS Form 205 provides a listing of all frequencies and their relevant agency assignments for each operational period during the incident. Often, ICS Form 205 summarizes information obtained from other sources, such as the Communications Resource Availability Worksheet (ICS Form 217A). If a local jurisdiction has developed a Communications Resource Availability Worksheet (ICS Form 217A), it will be contained within its Tactical Interoperable Communications Plan (TICP).

However, during some incidents, an ICS Form 217A or TICP may not be available. If this is the case, information about available frequencies may need to be collected from local sources, such as the local dispatch center or local communications point of contact (POC). Please refer to the Local Communications Point of Contact (POC) section, which appears later in this chapter.

It is good practice to create an ICS Form 205 and include the network currently in use as soon as you arrive. The COML should keep a personal copy of the ICS Form 205, which includes all of the assigned networks. This serves as a record for the After-Action Review (AAR) and is also a good starting place for creating a new Incident Radio Communications Plan for future operational periods.

In some cases, there may be a requirement for more networks than available channels permit. The COML should meet with the Operations Section to determine which frequencies might be shared.

Constructing an Incident Radio Communications Plan (ICS Form 205) can be made easier by asking a series of questions:

- Who is here?
- Who is coming?
- When are they arriving?

Next, place the agencies into functional groups and/or geographical divisions by asking the following:

- What is their assignment?
- Where are they doing their assigned tasks?
- When are they performing their assigned tasks?
- What equipment did they bring with them?

This knowledge, combined with a complete ICS Form 217A, should provide the COML with the necessary information to complete an ICS Form 205.

Notes:

- When creating an ICS Form 205, remember that users receiving the document are typically not technical. Do not use technical jargon unless it is essential. Keep it readable for the end user.
- List networks currently used for command and tactical purposes. Be sure only to list unclassified networks. Secure or secret networks and radios, such as those used by many National Guard units, should not be recorded on the official ICS Form 205.

Communications Resource Availability Worksheet (ICS Form 217A)

ICS Form 217A is a template that should be filled out before an incident. It allows agencies to enter their interoperable channels and talkgroups, providing essential information for communications planning during emergencies. The form includes details such as channel configurations, frequency bands, eligible users, and mode (analog, digital, or mixed mode). When properly prepared, it can save the COML time and minimize the possibility of mistakes on ICS Form 205.

Typically, ICS Form 217A is developed by the local jurisdiction in an administrative setting prior to the incident as part of the community's regular emergency planning. This document should include all public safety frequencies, channels, or talkgroups available (with established use agreements), regardless of agency, discipline, or ownership, with the understanding that you may need permission to use them.

Using electronic spreadsheet versions of ICS Forms 217A and 205 (e.g., Excel) allows lines to be copied from the pre-planned ICS Form 217A to the operational copy of ICS Form 205 (as the fields on ICS Forms 217A and 205 are the same).

Note: To see an example, please refer to the sample Communications Resource Availability Worksheet (ICS Form 217A) that appears at the end of this training guide.

Disseminating the Plan

The COML prepares ICS Form 205 and delivers it to the Planning Section. The Planning Section then uses this information in the Assignment List (ICS Form 204) and incorporates it into the IAP. Typically, the IAP contains multiple copies of ICS Form 204. It is essential for the COML to check all copies of ICS Form 204 for accuracy.

The COML should keep a separate master ICS Form 205, apart from the version submitted to the Planning Section, identifying all frequencies used during the incident, including Logistics frequencies and sensitive or confidential information, some of which may be excluded from the published version of the plan.

The COML will also ensure that a copy is delivered to the appropriate communications point of contact (POC) and any other regionally required personnel.

PACE Framework

The Primary, Alternate, Contingency, Emergency (PACE) is a decision-making framework used to ensure essential functions and activities can continue even in the face of disruptions or unexpected challenges. This framework will help the COML develop a sequence of alternatives to ensure the continuity of incident communications.

- **Primary:** The Primary option is the preferred or initial course of action for completing a task or achieving an objective. It represents the safest, most effective/efficient approach under normal operating conditions.
- **Alternate:** The Alternate option serves as a backup or secondary plan that can be implemented if the Primary option becomes unavailable or ineffective. It provides a viable alternative to maintain Continuity of Operations.
- **Contingency:** The Contingency option is a plan developed to address potential disruptions or “what if” situations that may arise during operations. It involves proactive measures to mitigate risks and ensure that essential functions can continue despite unforeseen challenges.
- **Emergency:** The Emergency option is the last resort and involves extreme measures to address critical situations or emergencies. It may involve activating emergency protocols, mobilizing additional resources, and taking decisive action to safeguard response personnel.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. Identify the different types of networks and describe their use.
2. When designing a radio system to support an incident, what factors should you consider?
3. Under what circumstances might the COML consider using commercial wireless or satellite services? Where can you obtain information about requesting such services?

Chapter 7: Coordination with Other Agencies

Emergency declarations at the federal, state, or local level can significantly affect the availability of resources to support the incident.

Learning Objective

At the conclusion of this chapter, you should be able to:

- Identify federal, state, and local resources outside of the IMT that can impact the COML's responsibilities and decision-making.

Federal Coordination

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (referred to as the "Stafford Act") authorizes the president of the United States to issue "major disaster" or "emergency" declarations before or after catastrophes occur. By making an emergency declaration, the president authorizes federal assistance to supplement state and local efforts in response to a threat or disaster.

Joint Field Offices (JFOs)

A JFO is a temporary federal facility that provides a central location for the coordination of federal, state, local, tribal, and territorial governments, the private sector, and NGOs with the primary responsibility for response and recovery. The JFO structure is based on the framework of the NIMS ICS and includes many of the branches in the functional sections parallel to those of the ICS structure.

A JFO is activated under the following circumstances:

- **Incidents of national significance:** When there is a need for a coordinated federal response to a major disaster or emergency.
- **Heightened threats:** During periods of increased threat levels, especially related to terrorism, a JFO may be established to preemptively coordinate response efforts.
- **Federal-to-federal support:** When federal agencies require coordination to support each other during specific incidents, such as chemical release accidents or spills of national significance.

The JFO interacts with the existing incident command structure in several ways:

- **Unified coordination:** The JFO operates using NIMS principles, integrating seamlessly with the local Incident Command Post (ICP) and ensuring unified command and control.

- **Resource support:** The JFO provides additional resources and support to the IC/UC on the ground, ensuring that logistical and operational needs are met effectively.
- **Information sharing:** The JFO facilitates the flow of information between on-scene responders and higher levels of government, enhancing situational awareness and decision-making.

The JFO's role is to support, not supersede, the authority of the local Incident Command. It ensures that federal assistance is coordinated effectively, aligns with local efforts, and enhances overall response capabilities.

Although the JFO brings its own complete internal communications systems, the COML should be aware of the JFO for several reasons. The JFO has access to specialized equipment and personnel that may be useful to the COML when setting up and maintaining communications systems.

How the COML interfaces with the JFO to request support may depend on the state or local jurisdiction. In general, requests for resources are sent through the local jurisdiction to the state's emergency management agency, which forwards the request to the federal government. This can be facilitated with an incident management software package or through a simple email chain.

If the JFO is integrated into the communications systems that the IMT is using, this will require the support of the COML, who would be responsible for representing the IMT during efforts to loop the JFO into local communications systems.

JFO/IMT coordination goes beyond the technical aspects of integrating communications systems. The COML and JFO can engage in information sharing to keep each other informed of any communications issues that may occur.

Emergency Support Function (ESF) Annexes

ESF Annexes are an integral part of the National Response Framework (NRF). ESF Annexes provide a structured framework for coordinating federal interagency support during emergency incidents.

These annexes outline the roles and responsibilities of federal departments and agencies, ensuring a coordinated and effective response. ESFs serve as mechanisms for grouping common functions required during incidents. State and local jurisdictions typically develop ESF annexes in their emergency plans as well.

Emergency Support Function 2 (ESF #2) – Communications

ESF #2 plays a critical role in disaster response and recovery efforts. Its purpose is to restore and coordinate communications during emergencies. ESF #2 focuses on the telecommunications and essential information needs of various entities, including state, local, tribal, territorial, insular areas, federal departments and agencies, non-governmental

organizations, industry essential service providers, private sector partners, and individuals. Responsibilities include disaster emergency communications, infrastructure support, coordination and planning, and information delivery.

ESF #2 ensures operable and interoperable voice and data communications, assists in restoring basic public safety communications infrastructure, and facilitates the delivery of mission-critical information. State and local jurisdictions typically develop the ESF #2 - Communications Annex as part of their emergency plans.

FEMA Disaster Emergency Communications (DEC)

The FEMA Disaster Emergency Communications (DEC) cadre deploys, installs, operates, maintains, and protects telecommunications and operations assets in response to all-hazards disasters and in support of planned special events. The DEC maintains and protects telecommunications equipment, facilitates interoperable communications, and aids in evaluating post-disaster communications needs. Regional FEMA DEC coordinators typically lead Federal ESF #2 teams during declared disasters.

Requests for DEC resources should go through the state's emergency management agency, which forwards a request for assistance from the federal government. If the DEC is deployed to an incident, they will use their internal communications systems, which should not cause interference with local operations. However, the DEC staff should be in contact with local agencies and the COML to ensure that no interference occurs.

Mobile Emergency Response Support (MERS)

The FEMA DEC cadre supports disaster emergency communications with six geographically dispersed Mobile Emergency Response Support (MERS) detachments and a pre-positioned fleet of Mobile Communications Office Vehicles. MERS resources can provide self-sustaining telecommunications, logistics, staff, and equipment that are immediately deployable to support a large disaster field office and multiple field operating sites within the disaster area.

FEMA Urban Search and Rescue (USAR) Teams

The National Urban Search and Rescue (USAR) Response System, established under the authority of FEMA in 1989, is a framework for organizing federal, state, and local partner emergency response teams as integrated federal disaster response task forces. Twenty-eight USAR task forces can be deployed by FEMA to a disaster area to assist in structural collapse rescue, or they may be pre-positioned when a major disaster threatens a community.

The task forces are equipped and ready to deploy within six hours in various response models. When federal support is anticipated prior to an event such as a hurricane, system

resources are often pre-positioned along with other federal responders to expedite support following the disaster.

USAR teams have their own spectrum and communications resources and do not generally release or share communications assets. Although they are self-sufficient, there may be a need for coordination to address interoperability issues if USAR is working alongside local resources.

Note: If USAR assets are deployed, USAR radio frequencies should be redacted from ICS Form 205.



For more information, please visit <https://www.fema.gov/emergency-managers/national-preparedness/frameworks/urban-search-rescue>.

USAR Incident Support Team (IST)

The USAR Incident Support Team (IST) is a part of the National Urban Search and Rescue Response System. It provides a group of highly qualified specialists who are readily available for rapid assembly and deployment to a disaster area. The IST provides federal, state, and local officials with technical assistance in the deployment and use of ESF #9 (Search and Rescue) resources through advice, incident command assistance, and management and coordination of USAR task forces.

The IST is developed to be consistent with the terminology and organizational structure of the National Response Framework (NRF) and NIMS. In a complex incident, the IST can be extremely helpful to a COML.

The IST can provide a rapid assessment of communications options, taking into consideration incident objectives, known status of existing communications systems and infrastructure, pre-positioned plans within the jurisdiction's Interoperability Communications Plan, and rapidly available options for communications equipment and supplies. This can significantly aid the COML in establishing effective communications plans and configuring resources. The IST also establishes logistics for the extended use of communications equipment in challenging environments, including the exchange and resupply of radios, phones, and computers for multiple shift changes. This logistical support can be invaluable to a COML during a complex incident.

State/Local Coordination

State/Local Emergency Management Agencies (EMAs)

State and local EMAs can support the COML in a variety of ways. EMAs can assist in allocating necessary resources, including personnel, equipment, and frequencies. They ensure that the COML has access to the required tools and support to establish and maintain effective communications during incidents.

These agencies can facilitate coordination among different responding entities and establish communications between various federal, state, and local agencies involved in the incident response. EMAs can assist the IMT with requests for federal resources. They can also assist in obtaining necessary permits and authorizations, such as Local Use Agreements (LUAs) and Special Temporary Authorization (STAs) from the FCC. This support ensures that all communications activities are legal and do not interfere with other communications systems.

EMAs may also provide technical support to troubleshoot and resolve any communications issues that could arise during an incident. This includes assistance with setting up communications equipment, programming radios, and managing communications systems. In addition, EMAs are often responsible for managing local or statewide alerts and warning systems.

The initial COML should reach out to the appropriate EMA as soon as they are notified and assigned to the incident. Upon arrival, the COML should reach out to the points of contact (POCs) within the EMA for additional information and possible assistance. At the conclusion of the incident, the COML should coordinate with these POCs to formally close out the incident and conduct an After-Action Review.

Emergency Operations Centers (EOCs)

EOCs provide critical infrastructure and resources for effective communications management. They provide a fixed, centralized location where communications strategies can be developed and coordinated. EOCs facilitate the integration of communications plans with overall incident response efforts, ensuring that all participating agencies are synchronized in their operations.

Furthermore, EOCs can provide access to advanced communications equipment and technical expertise. They ensure that the necessary technical infrastructure is in place, including backup power supplies, redundant communications systems, and internet connectivity.

In addition to technical and infrastructural support, EOCs can assist COMLs in obtaining and managing necessary communications resources, such as frequencies and equipment. They

help coordinate with state and federal agencies to secure Special Temporary Authorizations (STAs) and other regulatory approvals needed for the operation of communications systems.

EOCs play a vital role in information management by gathering, analyzing, and disseminating critical incident information to all stakeholders. This ensures that the COML has access to up-to-date information, which is essential for making informed decisions and maintaining effective communications during an incident.

The COML will most likely coordinate with the local communications POC rather than interact with the EOC directly.

State Urban Search and Rescue Teams (SUSARs)

A State Urban Search and Rescue Team (SUSAR) is a specialized unit that operates within a state's emergency management system to provide search and rescue services during disasters, emergencies, and other critical incidents. SUSAR teams are designed to be quickly mobilized and deployed to the scene of an emergency. They often work in coordination with local emergency services, state agencies, and federal resources.

Team members undergo rigorous training in various rescue techniques, including structural collapse rescue, confined space rescue, high-angle rescue, and water rescue. They are also trained in hazardous materials handling and disaster response operations. While SUSAR teams operate at the state level, they often collaborate with FEMA and the National Urban Search and Rescue Response System during large-scale disasters.

SUSAR teams bring their own communications support, including plans, personnel, and equipment. The IMT's COML should interface with the SUSAR to ensure they can communicate with the IMT. Frequencies and channels used by the SUSAR should be included on ICS Form 205.

Tactical Interoperable Communications Plans (TICPs)

A Tactical Interoperable Communications Plan (TICP) is a document that allows urban areas, counties, regions, states, territories, tribes, or federal departments and agencies to document interoperable communications governance structures, technology assets, and usage policies and procedures. It outlines interoperable assets available in a particular area, how those assets are shared, how their use is prioritized, and the steps individual agencies should follow to request, activate, use, and deactivate each asset.

During a complex incident, the TICP is used to facilitate effective and efficient communications among various agencies. The TICP helps to ensure that all agencies have a clear understanding of the available communications resources, how to access them, and the rules for their use. If a local jurisdiction has developed a Communications Resource Availability Worksheet (ICS Form 217A), it will be contained within the TICP.

The COML typically obtains the TICP during the initial response and assessment and also refers to it when developing the Incident Radio Communications Plan (ICS Form 205). The TICP can be obtained from the local communications POC, Emergency Operations Center, or dispatch center.

Statewide Interoperability Coordinator (SWIC)

The Statewide Interoperability Coordinator (SWIC) is a position established by FEMA to ensure effective communications and interoperability among different emergency response agencies within a state. The SWIC is responsible for coordinating and overseeing the implementation of statewide interoperability initiatives, particularly in the context of emergency communications. This includes:

- **Strategic planning.** Participates in the development, implementation, and maintenance of the Statewide Communication Interoperability Plan (SCIP), which outlines the strategy for improving emergency communications interoperability across the state.
- **Collaboration.** Works with various stakeholders, including state, local, tribal, territorial, and federal governments, emergency response groups, and private sector partners to ensure effective communications during emergencies.
- **Coordination.** Facilitates communication among various public safety entities, including law enforcement, fire departments, emergency medical services, and other relevant stakeholders, to ensure that these agencies can effectively communicate during emergency situations. The SWIC also serves as a point of contact for the federal government and industry on issues concerning statewide interoperable communications.

The SWIC may be a valuable resource to the COML for obtaining assistance with state or regional assets. Because SWICs also participate in the National Council of Statewide Interoperability Coordinators (NCSWIC), their contact information can be found on the CISA NCSWIC Membership website.



For more information about SWIC roles and responsibilities, please visit the CISA website at <https://www.cisa.gov/ncswic/swic-roles-responsibilities>.

To find contact information for the SWICs in each state, territory, or region, please visit <https://www.cisa.gov/safecom/ncswic-membership>.

Local Communications Point of Contact (POC)

Regardless of whether an incident is a declared emergency, one of the most important officials the COML must contact is the local communications point of contact (POC). This POC may have one of several different titles, such as Communications Coordinator (COMC) or Communications Duty Officer (CDO). At the local level, this could be the Radio System

Manager or the Communications Center Manager. At a state level, this could be the Statewide Interoperability Coordinator (SWIC) or state Communications Officer.

The local communications POC is responsible for maintaining contact with various local agencies that use radios and may potentially have to work together on an incident. The communications POC should also be knowledgeable about local equipment availability, such as pre-positioned equipment and cache locations. The communications POC collects this information and maintains awareness of local resources to assist the COML.

The communications POC will help with such tasks as assigning equipment and frequencies or talkgroups and may follow up on and keep track of the status of orders if local or state radio cache equipment is requested. The communications POC may also monitor adjacent units and incidents using similar resources or deconflict requests from adjacent incidents for the same assets.

Locally, the Communications Center Manager, Dispatch Center Supervisor, Local Frequency Coordinator, or Radio Systems Manager may function as the communications coordinator and coordinate local and regional communications assets.

This individual may also assist with:

- Equipment assignments.
- Frequency assignments (e.g., repeaters, links, aircraft, tactical).
- Status of orders (e.g., preorders, equipment, when ordered, ETA).
- Adjacent incident information (e.g., interoperability issues, frequency assignments, incident locations, contact information).
- Equipment availability (pre-positioned, cache location, shortages).
- Verifying incident location.
- Identifying if communications coordination assistance is available.

Before an incident occurs, the COML should work to build a network of contacts and stay familiar with local communications systems and coordinators. The COML should participate in planning meetings, training, and exercises where contact information for local coordinators is shared and updated. Further, the COML should have access to local, regional, and state communications plans that list points of contact and communications protocols.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. How can a COML leverage knowledge of federal, state, and local resources to integrate them effectively into their planning and operations?
2. How can understanding local resources outside of the IMT benefit a COML in fulfilling their duties more efficiently?

Chapter 8: The Incident Communications Center (ICC)

The Incident Communications Center (ICC) is a facility or defined area where incident communications systems are coordinated and managed. The ICC is responsible for establishing, maintaining, and operating all communications systems and equipment needed for the incident and ensuring that information is disseminated to the appropriate personnel.

The ICC is a separate entity from the Incident Command Post (ICP). However, the ICC may be located at or near the ICP or at a separate facility, depending on the needs and resources of the incident. The ICC is also completely separate from the Joint Information Center (JIC). If established, a JIC is a central location that coordinates media access and public information about incidents and emergencies.

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Identify important factors to consider when establishing the Incident Communications Center (ICC).
- Identify COML responsibilities at the ICC, including methods of organizing unit personnel.

Establishing the ICC

When establishing an ICC, consider the following:

- The location must be safe.
- The location should be near the ICP; however, they should not be co-located to avoid noise and distractions.
- The site must be large enough to ensure individual workstations do not interfere with one another and to accommodate for potential growth during the incident.
- The site must be located away from radio frequency and electronic noise, such as communication towers, refrigeration trucks, and electrical generators.
- The site should be close enough to the Incident Command Post and the Medical Unit for a quick exchange of information but separate enough to allow for a quiet environment in which communications personnel can adequately hear all voice traffic and other audible alerts.

- The ICC may have significant electrical power requirements and should be located close to a reliable electrical source.

Note: Depending on the scale of the incident, it is possible that more than one ICC may be established; however, this is extremely rare and is not recommended.

ICC Facilities

There are several physical forms an ICC can adopt.

- In urban and suburban environments, a school or commercial building may be considered, though the architecture of the building may obstruct long-range, low-penetration frequencies such as VHF low-band.
- In some situations, the ICC may be within the normal dispatch center for the local area. The dispatch center may handle all of the radio traffic as they would for normal day-to-day operations, or they may choose to assign a specific person to handle the incident dispatch.
- A mobile communications center (MCC), which is a large vehicle (similar to an RV) or a trailer with a variety of communications equipment already installed and equipped with other connections, such as data links, cell reception, and satellite feeds, may be used.
- A mobile command vehicle, which is like a mobile communications vehicle specifically designed to support command functions, may be used. Often, mobile command vehicles have a dedicated communications area that may be perfectly suitable for a COML's needs.
- In wilderness situations, a tent may be a suitable option, as it is the most a COML can expect, though these have the advantage of being mobile and relatively inexpensive.

Within the ICC, the COML must ensure workstations are installed to accommodate the various technologies utilized during the incident. There will need to be workstations for radios, telephones, and computers. The COML must also ensure that the ICC has adequate supplies, including ICS forms, copies of the IAP, and maps of the incident area.

Mobile Communications Centers

When considering an MCC, it is important to consider the vehicle's capabilities and ability to access the incident location. The COML should consider:

- The amount of space required for the vehicle.
- The route of travel the MCC must take to reach the site. Can it arrive safely? For example, can the vehicle clear underpasses or travel off-road?
- The space should be clear of any overhead obstructions that may interfere with the raising of a mast or other equipment.
- Whether the vehicle needs to be on a solid surface (e.g., blacktop).
- If satellites are involved, they will need a clear view of the sky. Some satellite services will require a view to the south.
- The power requirements for the MCC, which include the usage of shore power or a fueling plan for a generator.

Additionally, it is important to consider the capabilities of the MCC. FEMA Resource Typing can be helpful in determining capabilities, but it is important to remember to request what is needed. Sometimes, Type 1 MCCs are going to be the only option for the capabilities you need. At other times, a Type 2, 3, or 4 may still provide all of the required capabilities at a lower cost and with fewer logistical constraints.



For more information on FEMA Resource Typing, go to the FEMA Resource Typing Tool Library at <https://rtlt.preptoolkit.fema.gov/Public>.

Managing the ICC

The COML is responsible for establishing and managing the ICC. This includes obtaining required resources and, in some cases, training local personnel.

ICC responsibilities include:

- Determining staffing and equipment requirements.
- Operating radios and/or telephones.
- Relaying messages.
- Logging and documenting communications traffic.
- Monitoring emergency communications and facilitating radio system traffic when an emergency arises.
- Ensuring all ICC personnel are briefed on the ICS Form 206 (Medical Plan) and related procedures.

- Ensuring all ICC personnel are briefed on incident within an incident (IWI) procedures.

The ICC is also responsible for monitoring all radio traffic. Document radio and phone activities on the Communications Log (Form 309). Use the General Message (ICS Form 213) to communicate messages to the appropriate party and relay information back to the field. Although not required, logging recorders and instant playback recorders are recommended for capturing radio traffic.

For some fixed communications sites, consider that they may not be recording every channel. Tactical traffic is often not recorded. When utilizing a trunked radio system, all channels are usually recorded. Check with the local Radio System Manager to determine which channels are recorded. In the absence of a logging recorder, various scanner software vendors can provide this service.

Note: During some high-profile incidents, high-ranking officials or VIPs may decide to visit. In such cases, the presence of these individuals may potentially disrupt operations. Also, restrictions may be placed on communications due to operational security concerns.

Staffing and Equipment Considerations

When ordering personnel for the Communications Unit or the ICC, the COML should consider several factors.

These include operational hours and work schedules, such as whether the ICC will be staffed for a 24-hour operation and the size of the organization. Additionally, the COML should evaluate the amount of communications traffic expected, the duration of the incident or event, and the sharing of communications duties with local agencies.

It is also important to consider the qualifications for ordered resources, such as Emergency Medical Dispatch and Criminal Justice Information Systems (CJIS), as well as network configuration and security requirements.

During an incident, there is potentially more than one approach to requesting or ordering resources. It is important to know and understand the ordering forms or systems that your organization uses. Utilizing the General Message (ICS Form 213), Resource Request Message (ICS Form 213RR), or a similar form or system is recommended for properly managing resource orders.

It is recommended that separate forms be used for personnel and equipment requests.

Note: Whenever the COML orders resources (personnel or equipment), they should think ahead about when and how those resources will be demobilized later.

Communications Log (Form 309)

The Communications Unit may use Form 309 to manually record telephone and radio traffic. A logging recorder is faster and easier but may not be available on every incident.

Note: Form 309 is not considered a standard FEMA ICS form and is not included in the NIMS ICS Forms booklet; however, it can be found on various websites. Some versions include space for recording “message numbers.” Keep in mind that tracking message numbers can be challenging, particularly when numerous messages are being processed or when there is more than one communications specialist.

To see an example, please refer to the sample Communications Log (Form 309) at the end of this training guide.

Local Dispatch Center

During some incidents, it may be practical or necessary to involve local dispatch centers in managing communications traffic. Examples include:

- Dispatching local EMS resources to an incident.
- Coordinating local resources with incident resources where the local dispatch center needs to communicate with their personnel.
- Handling nighttime operations, such as having the local dispatch provide coverage instead of staffing night shifts within the ICC.

Managing Incidents Within an Incident (IWLs)

The Communications Unit is often a key component for dealing with an incident within an incident and must have specific protocols in place for dealing with such occurrences. If there is an IWI plan, it should be followed. If there is no IWI plan in place, the COML should discuss this with the LSC and ask that one be prepared.

Until an IWI plan is in place, ICS Form 206 should be followed according to how the Communications Unit will be involved in emergency medical situations. If the ICS Form 206 involves the Communications Unit but is not clear on procedures, the COML should address this with the Medical Unit Leader or Safety Officer and the LSC. It is important to note, however, that not all IWLs relate to medical emergencies.

The protocol should consider what information should be released over the radio if an IWI occurs. Dedicate appropriate airtime to an IWI, but remember that the primary incident response is still going on at the same time. Consider your ability to move this incident to a tactical channel. Situations may occur where providing care to responders (in contrast to those affected by the incident) becomes the priority.

Determine Supply Needs

The COML should ensure that the ICC is properly supplied. Take inventory to determine what supplies are on hand, what supplies have already been ordered, and what supplies have been brought to the incident by the Communications Unit staff. The COML should also determine if the hosting entity has a cache of radios, chargers, or spare batteries that can be issued to incident personnel.

Ensure that you have ordered supplies well in advance and in sufficient quantities to accommodate the anticipated growth of the incident and the projected number of personnel in the ICC.

Very few public safety agencies in the all-hazards world carry battery packs that hold AA batteries for radios, but these may be an option that could be stocked by an IMT or other communications resource.

During the early stages of an incident or event, or even beforehand if you are part of an IMT, it is essential to establish a policy that includes provisions for personnel (especially those in Operations, Safety, and Medical) to bring their agency-issued cell phones and portable radios along with chargers and spare batteries. However, it is crucial that their radios are programmed with the NIFOG interoperable channels before traveling to the incident or event.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. What are some key factors to consider when establishing an ICC, and how can they impact its effectiveness?
2. How can a COML ensure that the ICC is set up efficiently and meets the needs of the incident?
3. What responsibilities does a COML have at the ICC, and how can they effectively organize unit personnel?
4. From your personal experience, can you provide examples of successful ICC setups and the factors that contributed to their success?

Chapter 9: Transition and Demobilization

Learning Objectives

At the conclusion of this chapter, you should be able to:

- Identify the components of the Demobilization Plan and the steps involved in the demobilization process.
- Differentiate between demobilization and transition tasks.
- Recall the procedures for properly conducting an After-Action Review (AAR).

Transition Planning

Although most of the procedures are the same, there is a difference between transition and demobilization. During a transition, a new team arrives to replace the current Communications Unit. Depending on whether this group brings its own equipment, this could entail much less demobilization of equipment than actual demobilization.

When demobilizing or closing an incident, the incident itself is scaled down, and personnel and equipment are reassigned or released with the eventual termination of the incident in mind. When preparing for a transition (but not a full demobilization of communications assets), it is important to know if this transition is to another IMT or with the hosting jurisdiction.

If the incident is being handed over to another IMT, it may be necessary to transfer all or part of the communications equipment to the incoming IMT. Inventories must be accounted for, and the status of the equipment must be documented. It will need to be determined whether you or the incoming COML will arrange for the demobilization and shipping of any communications equipment or supplies that are no longer required. Ideally, you should offer to do this as the outgoing COML because it will help the incoming team as well as the records and reconciliation.

During the transition, the outgoing COML should brief the incoming COML about the status of incident communications systems. The outgoing COML should share any communications agreements, identify local POCs, and provide their contact information. High-cost items should also be identified in case the incoming team wants to set release priorities.

As part of the transition process, the outgoing COML should prepare a transition packet containing all relevant documentation gathered to date. If any members of the Communications Unit or the ICC under the supervision of the outgoing COML are going to remain at the incident, the outgoing COML should complete an Incident Personnel Performance Rating (ICS Form 225) for each of the remaining individuals and pass those on to the incoming COML with other transition documents.

If transitioning to the hosting jurisdiction, it will need to be determined if the jurisdiction will switch to their local communications systems or if they will need to retain any equipment or supplies that were used by your IMT. If the former, you will need to arrange for the demobilization and shipping of all communications equipment and supplies. If the latter, the transition would be the same as with another IMT.

Demobilization Considerations

Although the IC/UC establishes the date and time in which demobilization begins, demobilization is a constant process that begins upon arrival. As you order resources, including people, equipment, or frequencies, you should start planning on how you will release those assets when they are no longer needed.

Demobilization includes equipment and personnel demobilization as well as the rehabilitation of assets. Equipment and supplies should be returned to a ready state for the next deployment. Personnel should be properly rested before traveling.

The COML is responsible for the orderly demobilization of the Communications Unit, ensuring equipment is collected and accounted for and all Communications Unit documentation is completed and submitted to the Planning Section. As COML, you should consider these questions:

- What Communications Unit resources are to be released?
- When can the resources be released?
- Is the Demobilization Check-Out (ICS Form 221) ready for distribution?

Remember that deployed assets, such as radios, must be collected from everyone when they demobilize. However, deployed repeaters and other assets cannot be removed until communications activities depending on those assets are closed.

When the COML receives orders to begin demobilization, they must:

- Know the exact date and time of the planned demobilization and treat it as a deadline.
- Discuss incident priorities with other sections so that if demobilization occurs in a phased fashion, the operations of other sections will not be affected.
- Know, through discussions with their supervisor, whether the Communications Unit personnel and equipment will be transitioning elsewhere or if they will be released.
- Attempt to phase out of the incident by identifying supplies and personnel no longer required and releasing them accordingly.
- Consider work/rest regulations prior to demobilization and ensure all personnel are following established check-in/check-out procedures.

Remember that some resources, such as cache radios and repeaters, may need to be shipped back. Bills of lading and shipping notes may be required.

Note: If there is a Tactical Interoperability Communications Plan (TICP) in place, it may include SOPs for the return of equipment.

Demobilization and Check-Out

Upon receipt of the instructions to demobilize, which usually comes from the LSC, the COML must:

- Brief their staff on the demobilization procedures and the Communications Unit's responsibilities.
- Post a copy of the Demobilization Plan, emphasizing adherence to work/rest guidelines and establishing check-out procedures for crews and overhead personnel as they return their equipment and leave the incident.
- Ensure that accurate inventory is maintained, communications equipment is prepared for demobilization, and equipment is stored properly in preparation for shipment.

Many pieces of communications equipment will have their own established process for demobilization. The local communications POC will be able to help identify these procedures and release the equipment's frequencies. After these tasks have been accomplished, all documentation must be submitted to the Planning Section.

Demobilization Check-Out (ICS Form 221)

During demobilization, the COML should ensure that the Demobilization Check-Out (ICS Form 221) is complete. Personnel must often meet with the Communications Unit to return any communications equipment assigned to them and attest that they have checked in their equipment. If the Communications Unit box is checked, the Communications Unit must sign off that all equipment has been returned. For more information on ICS Form 221, refer to the ICS Training Reference Guide.

Incident Personnel Performance Rating (ICS Form 225)

During demobilization, the COML is also responsible for completing performance evaluations and the Incident Personnel Performance Rating (ICS Form 225) for each employee working under their direction. Before the person being rated leaves the incident, the COML should review the form with them, and both parties should sign it. The completed form is then delivered to the Documentation Unit.

It is important to note that for trainees, a copy of the completed ICS Form 225 must accompany their PTBs. Otherwise, the completed PTB may not be accepted. For more information on ICS Form 225, refer to the ICS Training Reference Guide.

Equipment Demobilization

The COML will be responsible for demobilizing any equipment they have utilized during the course of the incident. All equipment should be demobilized safely and efficiently. Ensure that equipment is rehabilitated and returned to a ready state as soon as possible (e.g., recharge batteries and return equipment to default settings). Ensure the facility is prepared for departure and that all equipment is accounted for. You also may be responsible for canceling any services that were requested during your time on the incident (e.g., additional phone lines, satellite services).

Gateway deactivation requires an announcement to be issued on shared channels stating that the gateway is being terminated. The announcement is issued by the radio operator for the incident based upon input from the COML acting in concert with the LSC, OSC, and IC/UC. Confirmation or acknowledgment must be obtained from all units using the gateway indicating that they are returning to their normal operating channels/talkgroups.

Regarding equipment demobilization, Tactical Interoperable Communications Plans (TICPs), if available, provide SOPs for the return of equipment, maintaining accountability and addressing any issues that arise. The COML should ensure that all final documentation is completed and submitted to the appropriate location.

Also, it is recommended that electronic documentation should be backed up with a paper-based system. Resource Status Cards (ICS Form 219), or T-Cards, provide a simple way to hand off to a replacement IMT who may not have computer capabilities. Additionally, a T-Card sign-out system has the benefit of capturing the signatures of persons to whom the equipment was assigned.

Transfer of Accountable Property

As the COML, you may be responsible for issuing pieces of equipment. Equipment that is under your control must be accounted for at all times. Therefore, it is important to ensure that proper documentation is completed anytime equipment or accountable property changes hands. Depending on the incident, the transfer of accountable property may occur in many different ways.

During some incidents, accountable property is returned to a centralized location and then reissued to the next person. Other incidents will allow for accountable property to be transferred directly from one person to another without it coming back to the centralized location. This may also depend on the type of equipment that is being issued.

For example, it is relatively easy to return a portable radio at the end of each shift. However, a portable repeater or other deployable equipment may be in place continuously to support critical incident communications. It may not be possible to take such equipment out of service simply to transfer the property. Work with your supervisor and the LSC to determine

the process for the transfer of accountable property and to complete the necessary documentation. Documentation may include hand receipts, T-Cards, check-in/check-out forms, or other tracking systems.

Demobilization Documentation

The COML is responsible for the following documentation:

- Incident Radio Communications Plan (ICS Form 205)
- Resource Request Message (ICS Form 213-RR)
- Communications Log (Form 309)
- General Message (ICS Form 213)
- Waybills
- Activity Log (ICS Form 214)
- Agency-specific forms
- Equipment logs
- Transition notes

All documentation must be submitted to the Documentation Unit at the end of the incident. If transitioning from the incident, make enough copies for your own records to submit to the Documentation Unit Leader and to provide to the incoming COML.

Note: Storage media for logging recorders may also become part of the incident record; however, the COML may not have control over this.

After-Action Review (AAR)

The COML is usually required to submit some kind of narrative of their activities throughout the incident at demobilization. When this occurs, it is often in the form of an After-Action Review (AAR). Originally taken from the military, this review consists of a comparison of what was intended to occur and what actually happened. In this format, improvements and constructive criticism can be more easily expressed, and particular things that “went wrong” or not according to plan can be highlighted for the next incident.

The AAR should be collaborative and instructive. Feedback and comments from subordinates are highly encouraged. The COML should conduct a “hot wash” with the Communications Unit staff before their release to gain feedback and comments. This information will be compiled into a report to be included in the AAR.

A hot wash is an informal, immediate debriefing session held at the end of an operational period or after an incident or exercise. It serves as a quick review of the actions taken during the operation or exercise to capture initial feedback on what went well and what could be improved.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. How does demobilization differ from transition, and how could these differences affect the COML's management of incident resources?
2. What steps should be taken to ensure all communications equipment is accounted for during demobilization?
3. Have you ever received a performance review after working on an incident? If so, can you provide examples of how Incident Personnel Performance Ratings have or will impact your performance in the field?

Chapter 10: Additional COML Resources

Learning Objective

At the conclusion of this chapter, you should be able to:

- Identify resources, services, and tools available to the COML and the Communications Unit.

Communication Assets Survey and Mapping (CASM) Tool

The Communication Assets Survey and Mapping (CASM) Tool, offered by the CISA Interoperable Communications Technical Assistance Program (ICTAP), is the primary resource nationwide for the emergency communications community to inventory and share agency, asset, and Communications Unit information for the purpose of planning public safety communications operability and interoperability.

CASM provides a real-time, geographic display of communications assets. This allows communications personnel to quickly understand what communications resources are available in a specific area, aiding in rapid deployment and utilization during an incident.

CASM helps in building a comprehensive situational picture by integrating communications asset data with other geographic information. This enhanced situational awareness allows for better decision-making and strategic planning during emergencies.



To find out more about CASM, log in, or request access, please visit <https://www.cisa.gov/safecom/casm-tool>.

For more information about the Interoperable Communications Technical Assistance Program (ICTAP), please visit <https://www.cisa.gov/safecom/ictapscip-resources>.

Commercial Wireless and Satellite Service Providers

Wireless Carrier Services

If you believe your incident or planned event will require additional wireless coverage or capacity, reach out to the wireless carrier. Commercial wireless carriers with deployable emergency resources include:

- FirstNet (AT&T) Response Operations Group (ROG)
- Verizon Response Team
- T-Mobile Emergency Response Team (ERT)

Please refer to the National Interoperability Field Operations Guide (NIFOG) for more information on the resources provided by these commercial carriers and how to order them.



For additional information on **FirstNet Response Operations Group (ROG)**, please visit <https://www.firstnet.com/power-of-firstnet/response-operations-group.html>.

For additional information on the **Verizon Response Team**, please visit <https://www.verizon.com/business/solutions/public-sector/public-safety/programs/verizon-response-team/>.

For additional information on the **T-Mobile Emergency Response Team (ERT)**, please visit <https://www.t-mobile.com/responsibility/community/emergency>.

Satellite Services

In some cases, sparse local resources may require atypical resource solutions. Commercial satellite providers and local telephone and data companies may offer solutions. For example, you may consider using low earth orbit (LEO) service providers, mobile and fixed satellite voice services, and push-to-talk (PTT) solutions. For more information on using satellite services, please refer to the National Interoperability Field Operations Guide (NIFOG).

Information Technology (IT) Providers

Two potential IT providers that the COML should be aware of include the Information Technology Disaster Resource Center (ITDRC) and the Cisco Crisis Response. Information about requesting these resources can be found in the National Interoperability Field Operations Guide (NIFOG).

The Information Technology Disaster Resource Center (ITDRC)

ITDRC is a nationwide, non-profit organization that leverages volunteers from across the technology sector to deploy solutions immediately following a natural disaster. It was founded in 2008 to provide communities with the technical resources necessary to continue operations and begin recovery after a disaster.

ITDRC maintains a distributed cache of communications equipment and surge technology assets to meet the short- and long-term needs of communities during response and recovery. Most resources are available for immediate deployment through their Mobile Technology Units, Tech Task Force (TTF), or National Disaster Relief Coordination Center (NDRCC).



For more information, please visit <https://www.itdrc.org/>.

Cisco Crisis Response

Cisco Crisis Response provides temporary, mission-critical voice, data, and video service to first responders, state, local, and federal agencies, critical infrastructure, and humanitarian aid organizations. Services may be provided for pre-planned and disaster incidents, subject to availability. This is a best-effort, pro-bono service.



For more information, please visit <https://www.cisco.com/c/en/us/about/csr/impact/cisco-crisis-response/incident-response.html>.

National Interagency Fire Center, NIFC National Interagency Incident Communications Division

The National Interagency Fire Center (NIFC) is located at the NIFC in Boise, Idaho, and coordinates between federal and state land management agencies, supplying portable communications equipment and systems to support incident communications. The NIICD is a partnership between the USDA Forest Service and Department of the Interior agencies. NIICD's mission is to provide portable emergency communications, technical training, and airborne remote sensing imagery services.

NIICD maintains a National Incident Radio Support Cache (NIRSC). The NIICD Cache System is designed to support land management incidents, namely wildfires. However, these

communications resources are designed to support any type of emergency or disaster, including those that are handled by an “all-hazards” IMT.

When NIICD radios are deployed to a non-wildland incident, they are typically requested through a state forestry agency, department of natural resources, Emergency Management Assistance Compact (EMAC), or other emergency management procurement process. However, to access and deploy cache radios and other resources from NIFC, agencies must have a prearranged reimbursable agreement in place. This ensures that the resources can be utilized effectively during incidents, particularly due to high demand and limited availability during peak fire seasons.

Also, the deployment of NIRSC radios requires the presence of an NWCG-qualified COMT or COML. NWCG qualifications are different from all-hazards qualifications.



For more information, refer to the *National Incident Radio Support Cache (NIRSC) User's Guide 2022* at

https://www.nifc.gov/sites/default/files/NIICD/docs/2022_NIRSC_User_Guide_Final_Webview.pdf.

Also, please visit <https://www.nifc.gov/resources/NIICD>.

The National Interoperability Field Operations Guide (NIFOG)

The National Interoperability Field Operations Guide (NIFOG) is a technical reference designed for emergency communications planning and for radio technicians responsible for radios that will be used in disaster response. It includes rules and regulations for the use of nationwide and other interoperability channels, tables of frequencies and standard channel names, and other reference material. The guide is formatted to be pocket-sized, providing quick access to crucial information during emergencies.

For a COML, the NIFOG is particularly important because:

- It serves as a comprehensive reference for establishing interoperable communications, which is essential during multi-agency responses to incidents.
- It helps in managing and coordinating communications resources effectively, ensuring that all responding agencies can communicate with each other.
- It provides guidelines on the use of interoperability channels, which is critical for the COML in setting up and maintaining clear communication lines during an incident.

The NIFOG is a useful tool that provides COMLs with information on the interoperability channels most likely to be programmed in the radios of responders from other disciplines or jurisdictions. This ensures that during emergencies, communication barriers are minimized and response efforts are better coordinated and efficient.

Note: Some references within the NIFOG are intended for wildfire responders and may be unfamiliar to individuals working within an all-hazards IMT.



To view or download a copy of the current NIFOG, please visit <https://www.cisa.gov/safecom/field-operations-guides>.

CISA Public Safety Library App

The Cybersecurity and Infrastructure Security Agency (CISA) has developed a mobile app called the Public Safety Library App to support emergency responders. This app enables public safety users to access current information electronically using their smartphones and other mobile devices, including electronic versions of:

- The National Interoperability Field Operations Guide (eNIFOG)
- The Auxiliary Communications Field Operations Guide (eAUXFOG)
- Other state and local field operations guides (FOGs)



To learn more about the Public Safety Library App, please visit <https://www.cisa.gov/safecom/public-safety-library-app>.

Priority Telecommunications Services (PTS)

Priority in communications is crucial to Continuity of Operations when facing adverse conditions such as weather events, mass gatherings, cyber-attacks, or events arising from human error. CISA offers three Priority Telecommunications Services (PTSs) that enable essential personnel to communicate when networks are degraded or congested:

- Wireless Priority Service (WPS)
- Government Emergency Telecommunications Service (GETS)
- Telecommunications Service Priority (TSP)



This suite of offerings is available to all personnel, from executive leadership to field personnel, with national security and emergency preparedness functions. For more information, please visit <https://www.cisa.gov/topics/emergency-communications/priority-services>.

In addition, CISA offers a free Priority Telecommunications Services “PTS Dialer” app. The PTS Dialer app provides a streamlined way of making

priority calls and easy access to WPS and GETS services. For more information about the app, please visit <https://www.cisa.gov/resources-tools/services/pts-dialer-app-gets-and-wps>.

Wireless Priority Service (WPS)

WPS is designed to provide prioritized cellular network access to authorized national security and emergency preparedness personnel during emergencies.

WPS was established to ensure that key government officials and emergency responders can communicate effectively during times of crisis when cellular networks might be congested due to high call volumes. It grants these users a higher probability of completing calls by prioritizing their cellular traffic. Subscribers who have been authorized to use WPS can dial a special access code before entering the phone number, which signals the network to give their call a higher priority over non-WPS traffic.

WPS is integrated with other priority services, such as the Government Emergency Telecommunications Service (GETS), which provides priority for landline calls. Together, WPS and GETS ensure that key personnel can communicate across both landline and cellular networks during emergencies.



For more information, please visit <https://www.cisa.gov/resources-tools/services/wireless-priority-service-wps>.

Government Emergency Telecommunications Service (GETS)

GETS is a national communications service that ensures the completion of phone calls for national security and emergency preparedness users during times of network congestion.

GETS is a national emergency telephone service that provides authorized users with priority access and prioritized processing in the local and long-distance segments of landline telephone networks, ensuring that calls from GETS users (national security and emergency preparedness personnel) are given priority over regular traffic during emergencies.

GETS is supported by all major service providers. GETS calls are not subjected to carriers' call restrictions like the general public when the network is congested. Subsequently, GETS will try another long-distance carrier if one is busy.

Please note that GETS does not mitigate cellular congestion and cannot be used for toll-free numbers.



For more information, please visit <https://www.cisa.gov/resources-tools/services/government-emergency-telecommunications-service-gets>.

Telecommunications Service Priority (TSP)

The TSP program consists of two components: restoration and provisioning. Supported by an FCC regulatory mandate, TSP establishes priority for the restoration and provisioning of national security and emergency preparedness circuits. TSP restoration priorities are applied to new or existing telecommunications services to ensure they are restored by telecommunications vendors before a non-TSP program user.

Note that TSP restoration assignments must be requested and assigned before a service outage occurs. In other words, a user cannot request restoration assignments for critical circuits after a natural or technical disaster strikes.

TSP provisioning priorities facilitate the priority installation of new telecommunications services by vendors in a shorter than normal time interval. However, this service cannot be used to compensate for inadequate planning on the part of the user.

With the exception of emergency provisioning orders, restoration orders are processed before new service provisioning orders. In all cases, the service order is expedited according to the service vendor's "best effort."



For more information, please visit <https://www.cisa.gov/resources-tools/services/telecommunications-service-priority-tsp>.

PTS Dialer App

CISA has developed a Priority Telecommunications Services "PTS Dialer" app for cellular phones to provide a streamlined way of making priority calls. The PTS Dialer provides easy access to WPS and GETS services.



For more information about the CISA PTS Dialer app, please visit <https://www.gwids.cisa.gov/apps/>.

Shared Resources (SHARES)

SHARES, or Shared Resources, is a 24-hour emergency communications program administered by the Department of Homeland Security's (DHS) National Coordinating Center for Communications (NCC). SHARES uses High Frequency (HF) radio to allow users with national security and emergency preparedness (NS/EP) missions to communicate when other methods are unavailable. SHARES members use existing HF radio resources to coordinate and transmit messages needed to perform critical functions, including those areas related to leadership, safety, maintenance of law and order, finance, and public health.

Membership in the SHARES program is voluntary. SHARES is available on a 24-hour basis and requires no prior coordination or activation to transmit messages. Members consult the SHARES Handbook to find stations, frequencies, and/or Automatic Link Establishment (ALE) addresses of participating organizations they need to communicate/coordinate with. Participating SHARES HF radio stations accept and relay messages until a receiving station is able to deliver the message to the intended recipient.



For more information, please visit <https://www.cisa.gov/resources-tools/programs/shared-resources-shares-high-frequency-hf-radio-program>.

U.S. National Guard

Civil Support Teams (CST)

National Guard Civil Support Teams (CSTs) are specialized units established primarily to respond to potential catastrophic events involving weapons of mass destruction (WMDs) and situations involving chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) hazards.

While the primary mission of the Civil Support Teams focuses on WMD response, a portion of that response capability includes communications resources. CSTs may operate their Advanced Echelon Vehicle (ADVON) and their Unified Communications Suite (UCS) vehicles for communications support. This support may involve land mobile radio, video conferencing, satellite communications, and access to the internet.

Check with your local team about their communications and other support capabilities. These teams can be reached through the state emergency management agency or the state National Guard Headquarters.

Homeland Response Force (HRF)

The Homeland Response Force (HRF) is a regionally aligned chemical, biological, radiological, nuclear, high-yield explosive (CBRNE) asset established to support and enhance local, state, and federal emergency managers in response to natural, man-made, or terrorist-initiated CBRNE disasters and additional hazards that result in a National Incident Management System (NIMS) construct. Nationally, there are 10 HRFs (one per FEMA region).

When directed by the proper authority and upon the consent of the Governor(s), the HRF alerts and assembles within six hours. Although their primary focus is on CBRNE response, they also have a communications function. The HRF can provide Data Network Satellite (SATCOM), including video teleconference and voice networks, radio communications in HF, VHF, and UHF bands, as well as crossbanding. They also can provide NIPRNet (non-secure) or SIPRNet (secure) networking capabilities.

Other Response Groups

Auxiliary Communications (AUXCOMM)

Auxiliary Communications (AUXCOMM) is an inclusive term used to describe the many organizations that provide various types of communications support to emergency management, public safety, and other government agencies. It also describes the services themselves. This includes, but is not limited to, amateur radio, military radio, and citizens band radio (CB).

Civil Air Patrol (CAP)

The Civil Air Patrol (CAP) is a civilian auxiliary of the U.S. Air Force that provides emergency services for state and local agencies, as well as the federal government. It is composed of volunteers who are prepared to assist in times of disaster, both in the air and on the ground:

- **Search and Rescue.** CAP conducts 90% of inland search and rescue operations in the U.S., as tasked by the Air Force Rescue Coordination Center and other agencies.
- **Disaster Relief.** They provide disaster-relief photography and support to local, state, and national agencies, helping with impact assessment and recovery efforts.
- **Transportation.** CAP transports time-sensitive medical materials, blood products, and body tissues when commercial resources are unavailable.
- **Communications.** Maintains an extensive VHF and HF communications network to support emergency operations.

CAP members receive training to FEMA standards, ensuring they are equipped to coordinate with other emergency response organizations.



For more information, please visit

<https://www.gocivilairpatrol.com/programs/emergency-services>.

Military Auxiliary Radio System (MARS)

The Military Auxiliary Radio System (MARS) is a program sponsored by the United States Department of Defense, which consists primarily of licensed amateur radio operators who assist the military with communications on a regional and national level when traditional communications systems are unavailable. MARS members, including those on active duty, reserve, and National Guard units, provide a valuable service by offering their radio communications skills during emergencies.

In emergency incidents, MARS operators can provide critical communications links for the Department of Defense and other federal agencies when normal communications channels are disrupted. They support humanitarian efforts and disaster relief by facilitating communications between different agencies and helping coordinate response efforts. This auxiliary communications network is especially crucial during complex catastrophes where telecommunications systems are denied or impaired.



For more information, please visit <https://marsradioglobal.us/>.

Salvation Army

The Salvation Army Team Emergency Radio Network (SATERN) includes a worldwide network of volunteer amateur radio operators and other communications specialists who may be mobilized to transmit emergency information during a disaster event. SATERN provides essential communications services to and from disaster sites around the world, particularly when infrastructure is disrupted or destroyed.

SATERN helps emergency responders by:

- Offering a reliable communications link during disasters when traditional systems fail.
- Assisting with the handling of health and welfare messages after events like hurricanes.
- Partnering with other emergency responders and disaster relief agencies to facilitate communications needs.

SATERN provides emergency communications support to the Salvation Army wherever needed on-site at the local level via VHF/UHF networks. During widespread emergencies (e.g., hurricanes, earthquakes, forest fires), the 14.325 kHz net becomes emergency traffic, and the Health and Welfare (H&W) Net provides tactical assistance to those on-site and handles outgoing H&W messages. The 14.325 kHz net is generally on the air from 1200Z to approximately 0100Z during times of widespread emergency.



For more information, please visit <https://centralusa.salvationarmy.org/usc/satern-program/>.

Team Rubicon

Team Rubicon is a veteran-led humanitarian organization that unites the skills and experiences of military veterans with first responders to rapidly deploy emergency response teams. They help emergency responders by providing timely and efficient support during disasters, leveraging their military experience to bring order and aid to chaotic situations. Their operations include disaster response, rebuilding efforts, and international work, often in collaboration with agencies like FEMA, to enhance preparedness, response, recovery, and other emergency management operations.



For more information, please visit <https://teamrubiconusa.org/>.

Pause and Reflect



Review the following questions and think about how the information you've learned in this chapter will help you assume the role of COML during an incident. Write down your responses and be prepared to discuss your answers during the FLEX portion of the course. Use extra sheets of paper if necessary.

1. What is the NIFOG? What types of information does it contain, and how does this information help the COML perform their duties? Please provide some examples.
2. Do you have a copy of the current NIFOG? If not, follow the directions in this unit for downloading the CISA Public Safety Library App to your phone or mobile device, and then use it to download the eNIFOG so that it is readily available to you during the course.

Sample Documents

Sample Communications Resource Availability Worksheet (ICS Form 217A)

COMMUNICATIONS RESOURCE AVAILABILITY WORKSHEET							Frequency Band	Description
Form 217A							VHF High Band	Liberty County Fire
Channel Config	Channel Name/Trunked Radio System Talkgroup	Eligible Users/Assignments	RX Freq N or W	RX Tone/NAAC	TX Freq N or W	Tx Tone/NAAC	Mode A, D, or M	Remarks
1 Repeater	CFD DISP	FIRE	151.44500 N	110.9	156.39500 N	110.9	A	
2 Repeater	CFD TAC 1	FIRE	151.35500 N	136.5	156.59500 N	136.5	A	
3 Repeater	CFD TAC 2	FIRE	151.26500 N	156.7	156.15250 N	156.7	A	
4 Repeater	CFD TAC 3	FIRE	151.11500 N	186.2	156.37500 N	186.2	A	
5 Repeater	CFD SPCL EVT	ALL	151.05500 N	182.8	156.27000 N	182.8	A	
6 Simplex	WFIRE21	FIRE	154.28000 N	NONE	154.28000 N	NONE	A	Public Safety Mutual Aid
7 Simplex	WFIRE22	FIRE	154.28500 N	NONE	154.28500 N	NONE	A	Public Safety Mutual Aid
8 Simplex	WFIRE23	FIRE	154.29500 N	NONE	154.29500 N	NONE	A	Public Safety Mutual Aid
9 Simplex	WCALL10	FIRE	155.75250 N	NONE	155.75250 N	156.7	A	National Interop Channel
10 Simplex	VTAC11	FIRE	151.13750 N	NONE	151.13750 N	156.7	A	National Interop Channel
11 Simplex	VTAC12	FIRE	154.45250 N	NONE	154.45250 N	156.7	A	National Interop Channel
12 Simplex	VTAC13	FIRE	158.73750 N	NONE	158.73750 N	156.7	A	National Interop Channel
13 Simplex	VTAC14	FIRE	159.47250 N	NONE	159.47250 N	156.7	A	National Interop Channel
14 Repeater	LCPW ROADS	PUB WRKS	153.22750 N	136.5	155.25000 N	136.5	A	Interop w/ Public Works
15 Repeater	LCPW WATER	PUB WRKS	155.65250 N	136.5	154.99500 N	136.5	A	Interop w/ Public Works
16								
17								
18								
19								
20								

The convention calls for frequency lists to show four digits after the decimal place, followed by either an "N" or a "W", depending on whether the frequency is narrow or wide band. Mode refers to either "A" or "D" indicating analog or digital (e.g. Project 25) or "M" indicating mixed mode. All channels are shown as if programmed in a portable or mobile radio. Repeater and base stations must be programmed with the Rx and Tx reversed.

Sample Communications Log (Form 309)

Communications Log (ICS 309)

[illegible]

ICS 309-CAN