

COMMUNICATIONS

1. GENERAL

a. Fast, reliable, and accurate communications are essential for nuclear weapon accident or incident response operations. Moreover, securing adequate internal communications to support activities at the accident scene is a time sensitive operation. Equally critical to effective C2 is the timely establishment of external communications to higher levels, particularly in the Washington, D.C. area. The communications officers of the DoD IC must act immediately to ensure that appropriate communications equipment is identified and requested early in response operations. Information must be accessible. In general, the value of information increases with the number of users.

b. Effective response to a nuclear weapon accident or incident relies heavily on a communications officer's knowledge of secure and non-secure tactical, strategic, and commercial communications systems. He or she must be able to apply conventional and imaginative methods and ensure that required communications are available. He or she should be equally adept at establishing communications support in remote locations or in areas near existing communications systems.

c. The DoD, DOE/NNSA, FEMA, State, and/or civilian officials shall all establish their own internal communications systems at the accident or incident site and shall ensure that these systems are interoperable with those of sister agencies.

2. SPECIFIC REQUIREMENTS

The DoD IC requires internal communications with the operations center and forces in the field to control and keep abreast of response activities. External communications with higher levels of command are necessary to keep key personnel informed. Many initial communications requirements may be met by unsecured voice communications; however, both secure voice and record communications are required early in the response period. Communication requirements:

a. Establish the following communications capabilities internal to the accident site:

(1) Telephone communications between fixed site locations, for example, the operations center and the JIC/CIB.

(2) Field communications for EOD operations. Secure communications are always necessary.

(3) Wireless Communications. Provide secure wireless nets such as UHF/VHF nets for command, weapons recovery operations, radiological operations, security, and public affairs.

(4) Establish and assign radio call signs.

(5) Establish a local computer network or access to a local computer network. If possible, establish virtual C2 requiring password access. The computer network should be

protected by an appropriate firewall and be able to access the Internet, accommodate e-mail, and ease document processing storage and recovery. Additionally, computer assets must be robust enough to securely maintain the potentially large amount of records which will be generated during all phases of the response operation.

b. Establish the following external communications to higher HQ:

(1) The Department of Defense will establish telephone communications with the Combatant Command's Operations Center, the Joint Field Office (if activated), the Service Operations Center, the NMCC/JNAIRT, and the Office of the ASD(PA). DOE/NNSA actions will include establishing telephone communications with the appropriate Site Offices and the DOE. Conferencing may suffice early in the response.

(2) Multiple secure and non-secure telephone lines to support response force elements. The telephone network should be sized to ensure an adequate ability to handle the expected volume of traffic. The communications officer should consider programming the serving telephone switch or switches to increase the likelihood of call completion. Hunt groups should be considered and features, such as call roll over and voice mail, enabled where appropriate. DSN access must be considered.

(3) Secure voice through satellite, telephone, or high frequency (HF). Often using Secure Telephone Unit (STU) IIIs and Secure Terminal Equipment (STEs) shall be the most practical and immediate method of establishing secure voice.

(4) Access is required to the Defense Information System Network for record communications from remote locations.

(5) Internet access. The requirement to send and receive large data size documents and images between command authorities is probable. Therefore, Internet access should be as robust as practical. The communications officer should strive to provide bandwidth at 128Kbps or higher. SECRET Internet Protocol Router Network (SIPRNET) access is always desirable. If SIPRNET is available, the DOD IC and staff should consider the regular use of the SIPRNET chat room feature for keeping all concerned parties updated on the nuclear weapon accident response operation.

c. Coordinate frequency usage with all response organizations and with the NCS/ESF#2 representative to prevent interference and to ensure electromagnetic emissions will not create explosive hazards or affect electronic and field laboratory instruments. Get frequency clearances, as necessary.

d. Prepare the Incident Communications Plan and Signal Operating Instruction (SOI) for use by all response organizations.

e. If required, request the Chairman of the Joint Chiefs of Staff's deployable communications assets.

f. If required, get leased commercial communications.

g. If present, coordinate all communications activities and planning with the Federal Emergency Communications Coordinator (FECC), who is the lead person on ESF#2. The FECC is the single Federal point of contact in the accident or incident area to coordinate the Federal telecommunications requirements and industry's response. The FECC coordinates with the State telecommunications officer to ensure Federal communications requirements do not conflict with State needs. The FECC prioritizes conflicting requests and recommends solutions to the JFO Coordination Group.

3. RESOURCES

Communications capabilities and resources for nuclear weapon accident or incident recovery operations vary widely. Resources are as familiar as the telephone or as sophisticated as satellite capable secure voice radio. Communications assets must be able to deploy and operate in remote locations. This section briefly describes a variety of communication resources for response organizations. Because the same equipment supports many contingencies, only those assets required for a specific nuclear weapon accident or incident response effort should be requested. Resources are available from the Department of Defense, other Federal agencies, and commercial sources.

a. Service Assets. The Military Services maintain communications assets organic to combat support units and for contingency assets. Information about specific assets, as well as procedures for requesting and tasking Service assets, may be obtained from the respective Service operations centers or operational commanders. Service assets may be obtained by contacting the individual Service Operations Center.

(1) U.S. Army. U.S. Army Signal organizations are designed to support deployed forces from the theater Army level down to the smallest unit. Major communications support includes C2, communications, and automation systems. Essential elements of these areas include long haul transmission systems Super High Frequency (SHF) and Ultra High Frequency (UHF) satellite terminals, voice (Mobile Subscriber Equipment and Tri-Service Tactical [TRI-TAC] Voice Switches), record communications traffic (e.g., TRI-TAC Message Switches), Frequency Modulation (FM) and HF radio systems (e.g., SINCGARS), and data communications networks.

(2) U.S. Air Force. Tactical communications assets are available from both the Combat Communication Groups and HAMMER ACE. HAMMER ACE is a rapidly deployable team with military and commercial off-the-shelf technology communications equipment. The mission of HAMMER ACE is to provide initial secure C2 communications.

(3) U.S. Navy. The Joint Maritime Operations Command Center, Mobile Integrated Command Facility, and the Mobile Ashore Support Terminal comprise the U.S. Navy's Joint Maritime Command Information System, i.e., the U.S. Navy's tactical ashore communications capability. These systems were fielded to replace the Ashore Mobile Contingency Communication System. Although these capabilities primarily support the naval component commander of a Combatant Command or Joint Task Force, their modular organization makes these systems ideally suited for use with liaison teams or in support of contingency requirements.

(4) U.S. Marine Corps. Present Marine Corps C2, communications, computers, and intelligence systems mix some analog transmission equipment with digital transmission and

switching equipment that is compatible with TRI-TAC. During contingency operations, and if approved by the supported Combatant Commander, the Marine Air Ground Task Force HQ may extend Defense Information Infrastructure (DII) common users services (Internet Protocol Router, DSN, Secure Voice Systems, Defense Messaging System/Automatic Digital Network) through a DII entry point by way of a Ground Mobile Force satellite link.

b. Joint Chiefs of Staff Controlled Assets. Joint Chiefs of Staff contingency support communications resources are requested according to procedures in the Chairman of the Joint Chiefs of Staff Instruction 6110.01A (reference (bb)). Additional information on these assets may be obtained from the Joint Staff Contingency Support Division.

c. DOE/NNSA Assets. The DOE/NNSA maintains emergency response, air transportable communications services, and hardware. Systems include a multi-point telephone switch, fax, HF/VHF radio networks (with pagers), video teleconferencing, and terrestrial microwave system. A multi-channel satellite system is available to provide long-haul transmission capability. Single-channel International Marine Satellite (INMARSAT) terminals with data interface are included for advance party use and emergency backup. Secure communications include voice, fax, still and full motion video, and data. Field communications are linked into the DOE/NNSA ECN through satellite. DOE/NNSA assets may be obtained through the DOE HQ/EOC.

d. DHS Assets. DHS provides communications support in two primary ways – FEMA deployable assets and activation of Emergency Support Function #2.

(1) FEMA Assets. Telecommunications can be provided for one or multiple locations within a disaster location. This support is provided by Mobile Emergency Response Support (MERS) and Mobile Air Transportable Telecommunications System (MATTS) telecommunications assets which are based at five locations designed to support the ten FEMA regions (see Table 1.); further, Table 2. lists other communications assets which can be deployed by FEMA. Both MERS and MATTS can establish or reestablish communications connectivity with the public telecommunications system or Government telecommunications networks. They can interconnect facilities within the disaster region. MERS and MATTS can wire austere facilities and install computer, telephone, and video networks. Both systems have these telecommunications transmission capabilities:

(a) Satellite. Ku-band satellite for quick connectivity that provides up to 48 lines for either telephones or data. INMARSAT and American Mobile Satellite Corporation (AMSC) satellite terminals provide immediate, single-voice channel capabilities.

(b) Line of Sight Microwave. Microwave transmission to connect to the public network, provide connection to other facilities, or extend communications.

(c) High Frequency (HF) to communicate with Federal, State, and local emergency centers via the FEMA National Radio Network and FEMA Regional Radio Network.

(d) Very High Frequency (VHF) and Ultra High Frequency (UHF) for local radio communications.

Table 1. MERS and MATTS Regional Responsibilities

MERS or MATTS	Area of Responsibility
Maynard, MA MERS Detachment	FEMA Regions I and II
Thomasville, GA MERS Detachment	FEMA Regions III and IV
Denton, TX MERS Detachment	FEMA Regions VI and VII
Bothell, WA MERS Detachment	FEMA Regions IX and X
Denver, CO MERS	FEMA Regions V and VIII
Berryville, VA MATTS	As required

Figure 1. FEMA Regions



Table 2. Additional FEMA Assets

Type	Purpose
Fiber optic cable	Inter-site communication distribution
Private Branch Exchanges (MERLIN and G3) and telephones	Telephones and switches capable of supporting 25-300 people
Multiplexers (IDNX and IMUX), D4 channel banks, routers, and file servers	Communications routing and exchange
Personal computers with standard software configured in local and wide area networks	For use by the Federal responders
VHF and UHF radios	For local radio networks. These can be extended with repeaters
Video broadcast	To record and disseminate video information from the disaster location
INMARSAT and AMSC satellite telephones	Provide single channel voice or data

(2) ESF #2 Assets. While a full description of ESF #2 capabilities is available in reference (c), ESF #2 has the capability of providing access, when and where appropriate, to national-level programs such as the Shared Resources (SHARES) High-Frequency Radio Program, Telecommunications Service Priority (TSP) Program, Government Emergency Telecommunications Service (GETS), and Wireless Priority Service (WPS).

e. Commercial Assets. In the CONUS, acquisition of supporting communications systems from commercial carriers (for example, American Telephone and Telegraph) is possible. Commercial carriers may provide communications to a remote area by transportable microwave, carrier systems, or cable. Leased services, including telephone, data Teletypewriter Exchange, Telephone Exchange, and Wide Area Telephone Service (WATS), are available in most locations.

4. CONCEPT OF OPERATIONS. Nuclear weapon accidents and incidents present a variety of technical, logistical, and operational communications problems. Several factors, including the location of the accident, the response force involved, and the C2 arrangements of those forces, contribute to the complexity of the problems. This concept of operations focuses on the actions of the military response force(s) communications officer(s) and the DOE/NNSA communications personnel. The approach is to present items of concern sequentially, regardless whether the IRF, RTF, or DOE/NNSA communications officer takes the action. The RTF communications officer shall find out what has been accomplished before arrival and carry on from that juncture.

a. Initial Actions. The initial task of the response force communications officer is to determine the communications assets at, or close to, the accident or incident site. The local telephone company, State and/or local officials, or civilian authorities may provide information on the communication infrastructure near the accident or incident scene and the capabilities for

long haul and local communications; this information is particularly important if the accident or incident damaged or destroyed portions of the communication infrastructure. Additionally, cell phone capabilities may be severely limited in a large scale accident due to over usage. Once existing capabilities are determined, the communications officer should use these resources with deployed assets to establish an effective communications network.

(1) In remote or sparsely populated areas, the initial communication capability may consist of only hand-held, short-range VHF/FM radios, portable HF radios, cellular telephones, or wire (field phones). Conversely, if an accident or incident occurs close to a populated area, a coin-operated telephone, cellular telephones, or even a business or private telephone may be available immediately for emergency use. In either case, additional leased communications, such as Wide Area Telephone Service (WATS), may be obtained to supplement available communications. Because more time is required to provide leased assets to remote areas, the requirements must be identified and requested at the earliest possible time. Follow-on deployment of mobile communications provides the response force with additional local telephone and radio, as well as long haul secure voice and record capabilities.

(2) Another method of communications for external (long haul) communications, particularly if assets are limited, is the telephone conferencing capability of the Service Operations Centers, the NMCC, and the DOE/NNSA HQ/EOC. Further, if communication may be established from the site to the DTRA Operations Center and the DOE/NNSA Service Center, the DTRA Operations Center or the DOE/NNSA Service Center will assist by relaying information or coordinating with other forces and/or Agencies.

(3) The DoD IC may spend considerable time away from the Command Post. The response force communications officer must, therefore, plan communication methods to support the mobility of the DoD IC. Radio nets provided for DoD IC communications should have sufficient range and be capable of frequent use. If possible, the net should be secure and have a radio and/or wire integration capability into the local switchboard and long haul voice circuits. The staff directors for operations, planning, and logistics, as well as the special staff advisors, should be included in this net.

(4) The communications officer must take prompt action to get frequency clearances. Radio frequencies are managed at the national level by the Military Communications-Electronics Board (Joint Frequency Management Office). Each Service has membership on the board. Moreover, each Military Department has a frequency management office, but in most cases these offices have delegated the authority to assign frequencies to area coordinators. Additional details may be obtained from USA FM 24-2 or AFI 33-118 (references (bc) and (bd)). DOE/NNSA and FEMA communications personnel should coordinate frequency requirements through their own channels and keep the military communications officer advised. Failure to get valid frequency authorizations might result in interference with other critical communications.

(5) One of the more complex problems facing the response force communications officer is preparing an Incident Communications Plan (ICP) using the ICS205 form (see Figure 2.), as well as a Signal Operating Instruction (see Figure 3. for an SOI outline). The ICP should be designed to make the most efficient use of the communications equipment and facilities assigned to the accident or incident response operation. The SOI should be an easy-to-use instruction containing the capabilities and limitations of equipment and detailed "how-to-use" procedures for all available systems. The SOI should be unclassified, if possible, and widely distributed. It

should at least include system descriptions (charts and diagrams are helpful), an on-site telephone directory, dialing and telephone routing instructions, message addresses, message handling instructions and routing indicators, radio procedures and call signs, secure voice procedures, and Communications Security (COMSEC) operations security procedures, including Essential Elements of Friendly Information (EEFIs).

(6) Although COMSEC instructions are a part of the SOI, COMSEC deserves additional emphasis. Enemy or dissident elements may be able to intercept and exploit C2 communications systems and traffic used for response to nuclear weapon accidents or incidents. Compilations of individually unclassified items concerning weapons communicated during recovery procedures may well be classified, and unfriendly elements may be able to compile these items; therefore, the communications officer in conjunction with the Operations and Plans Sections, must plan to defeat this threat by determining the EEFI for the operation, and then acting to prevent interception or exploitation of this information. COMSEC actions to prevent exploitation of EEFIs may include using secure transmission facilities, communications discipline, codes and authenticators, and changing call signs.

Figure 2. Incident Communications Plan

INCIDENT COMMUNICATIONS PLAN				1. Incident Name	2. Date/Time Prepared	3. Operational Period Date/Time
Telephone						
4. Communications Plan Concept of Operation						
5. Contact List						
Section & Position	S T A T E	F E M A	O F A	Name	Phone Number	Cell Phone Number
Incident Facilities						
Command Staff						
General Staff						
Other FCO/SCO Staff						
ICS 205-A FEMA	6. Prepared by Date/Time				7. Reviewed by Date/Time	

Figure 3. Signal Operating Instruction

Signal Operating Instruction (Sample Contents)	
SECTION 1 - Communications Security	
SECTION 2 - Telephone Communications.....	
Figure 2-1: Telephone Routing Diagram	
Figure 2-2: Hot Line Routing Diagram.....	
SECTION 3 - Message Communications Instruction	
Figure 3-1: Message Example.....	
Figure 3-2: Eyes Only Message Example	
SECTION 4 - Radio Communications Instructions	
ANNEX A - Response Force Traffic Diagram	
ANNEX B - Telephone Numbers and Message Addresses	
B-1 - Tie Line Network Dialing Instructions	
B-2 - On-Site Telephone Diagram	
B-3 - Off-Site Contact Telephone Numbers and Message Addresses.....	
B-4 - Intercom Systems.....	
Intercom #1	
Intercom #2	
Intercom #3	
Intercom #4	
ANNEX C - Radio Call Signs.....	
Net #1 Grader	
Net #2 Looker	
Net #3 Catcher	
Net #4 Ivory	
Net #5 Blue	
Net #6 Angel	
Net #7 Red	
ANNEX D - Distribution.....	

b. Follow-On Actions. As additional response forces deploy to the accident or incident scene and a support base camp is established, additional communication resources shall be

deployed or acquired concurrent with the buildup. As this buildup occurs, the response force communications officer should establish and maintain a list of communications assets and capabilities on-scene. The list should include assets and frequencies belonging to non-DoD or DOE/NNSA agencies, identifying potential mutual interference, and should ensure that all possible assets are considered when meeting overall communication requirements. Coordination should be made with the appropriate representative from Federal and civilian authorities and/or officials having on-scene communication systems.

(1) As stressed throughout this chapter, increasing the quantity of communications assets and routing those assets into the appropriate users' hands is very important as the response organization grows. Additional communication assets, primarily in the form of telephones and VHF/FM radios, are needed for effective operation of the JIC/CIB and to support radiological monitoring and SR operations.

(2) As the response operations peak, so shall the communications support required. As the response transitions into SR, the primary communications should be routine situation reports, Military Standard Requisitioning and Issue Procedures messages, and other administrative messages. After the weapon(s) and weapon components are removed from the site, little or no need shall exist to communicate by secure voice; however, a record of communications support provided on-site during the early response and weapon recovery should continue through SR. This record should be submitted to the Documentation Unit of the Planning Section at the termination of the operation.