National Incident Management System

Information and Communications Technology Functional Guidance

August 2022

FEMA

This page intentionally left blank.

Table of Contents

Introduction

1. Purpose

The *National Incident Management System (NIMS): Information and Communications Technology Functional Guidance* provides a framework to incorporate Information and Communications Technology (ICT)[1] services within the Incident Command System (ICS) to meet the increasing demands and expectations for ICT capabilities.

This Guidance establishes how the ICT function manages the infrastructure and systems that support and enable communications, information management processes and applications required by an incident management's organizational structure. Additionally, this Guidance describes how the ICT function safeguards incident operations from cybersecurity threats and explains how to manage the inter-relationship of communications and information technology (IT) infrastructure. This Guidance does not describe the operational response to cybersecurity incidents.

This Guidance also describes the Incident Commander/Unified Command or Emergency Manager's authority to organize the ICT Branch based on incident complexity.[2] Additionally, this document explains the organization of and roles and responsibilities of the ICT function within an ICT Branch. This Guidance also introduces new ICT positions intended to support successful outcomes by providing communications resources and access to IT capabilities for Incident Commanders/Unified Command and Emergency Managers. While this Guidance incorporates the ICT Branch within ICS, the ICT Branch can be incorporated into any command and coordination system, such as the Incident Support Model[3].

Definition of Information and Communications Technology

ICT is broadly used to address the evolution and convergence of traditional telephone and radio with IT systems.

According to the National Institute of Standards and Technology (NIST), ICT encompasses "the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information."

[1] National Institute Standards and Technology (NIST) at: https://csrc.nist.gov/glossary/term/information_and_communications_technology

[2] National Incident Management System Incident Complexity Guide: Planning, Preparedness and Training available online at https://www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf

[3] National Incident Management System (NIMS), Appendix B EOC Organizations at: https://www.fema.gov/emergency-managers/nims.

2. Background

Since NIMS ICS was established in 2004, the complexity of communications resources has expanded significantly. In 2004, communications support focused on providing radio and telephone services and equipment to incident response and recovery personnel. Since then, incident management has increasingly relied on new capabilities, including IT and cybersecurity, to share real-time decision support and situation awareness information. The rapid emergence of new technologies and reliance on them poses a risk, as these technological systems are vulnerable to the threat of cyberattacks, and failure to protect communications and information sharing systems can be detrimental to disaster relief.

In response to evolving information and communications technology, the 2017 NIMS ICS clarified that the Communications Unit is responsible for establishing voice and data networks.[4] Recent incident response efforts revealed that the functional requirements to establish, manage and secure ICT for a large and complex incident may be beyond the manageable span of control of the traditional Communications Unit. The flexibility for the Incident Commander/Unified Command or Emergency Manager to establish an ICT function within ICS recognizes this concern and the need for a scalable framework to address increased ICT needs during incident response and recovery.

3. Applicability and Scope

For the scope and applicability of this document, please refer to the "Applicability and Scope" section of *NIMS*.[5]

4. Document Management and Maintenance

The Federal Emergency Management Agency's (FEMA) National Integration Center (NIC) is responsible for the management and maintenance of this document. Comments and feedback from stakeholders regarding this document should be directed to FEMA NIC at FEMA-NIMS@fema.dhs.gov.

[4] National Incident Management System (NIMS), Chapter IV Communications and Information Management at: https://www.fema.gov/emergency-managers/nims.

[5] National Incident Management System (NIMS) at: https://www.fema.gov/emergency-managers/nims.

Overview of Information and Communications Technology

One of the three major components of NIMS[6], Communications and Information Management describes the systems and methods that ensure incident response and recovery personnel, and other decision-makers have the tools and information they need to make and communicate decisions. Incident response and recovery personnel use ICT resources to communicate with one another, collaborate on response and recovery activities and assess the impacts and consequences of the incident. The ICT function supports NIMS by integrating voice, data and video communications capabilities.

1. The ICT Function

The ICT function establishes, maintains and protects the IT infrastructure, communications and IT capabilities utilized by other functional areas within ICS. The main responsibilities of the ICT function include:

- Setting up and maintaining the IT and communications infrastructure to support incident response and recovery personnel;
- Enabling integrated communications to provide and maintain contact among incident resources, enable connectivity between and among various levels of government and responders, establish and maintain situational awareness, and facilitate information sharing;
- Protecting IT and communications infrastructure deployed to support incident management, including, but not limited to, geographic information systems (GIS), social media, alert and warning systems and unmanned aerial systems as well as evolving communication types such as from citizenry;
- Liaising with cooperative IT departments from supporting jurisdictions; and
- Developing plans to ensure the necessary equipment, systems and protocols are in place to achieve integrated voice, data and video communications.

Though the ICT function is responsible for providing the pathway and access to networks and resources, it does not establish the policies and practices concerning how and when data is shared, or systems are utilized. The ICT function is responsible for implementing and complying with established policies.

[6] The National Incident Management System (NIMS) provides a comprehensive approach to coordinating personnel, organizations, resources and tactics to prevent, protect against, mitigate, respond to and recover from incidents. For more information, see: FEMA, National Incident Management System. October 2017. For more information, visit the website at https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

The ICT function executes its responsibilities in alignment with the four principles of Communications and Information Management:

- **Interoperability:** Interoperable communications systems enable personnel and organizations to communicate within and across jurisdictions and organizations via voice, data and video systems in real time. Interoperability plans address governance, standard operating procedures (SOP), technology, training and exercises and usage during routine operations and major incidents.
- **Reliability, Scalability and Portability:** Regular use of ICT systems helps ensure that they are familiar and acceptable to users, readily adaptable to new technology and reliable in any situation.
    - **Reliability** is the ability of a system to function in any type of incident, including within a single jurisdiction or agency, or within multiple jurisdictions with multiagency involvement. This allows for rapid deployment and response in incidents.
    - **Scalability** is the ability of a system to expand to support incidents of varying complexity—including a major incident or several incidents involving numerous responders and support personnel from multiple jurisdictions and organizations—and quickly increase the number of users on a system.
    - **Portability** is the standardization of technology and equipment. For example, the standardized assignment of radio channels across jurisdictions allows incident personnel to participate in an incident outside their jurisdiction. Portable technologies and equipment ensure the effective integration, transport and deployment of ICT systems without fixed infrastructure.
- **Resilience and Redundancy:** Resilience is the ability of systems to withstand damage and continue to perform after the loss of infrastructure. Redundancy is the applied duplication of services and enables the continuity of communications through alternative methods. Permanent infrastructure (e.g., municipal IT networks) and field-constructed systems (e.g., computer network in a joint field office) should both be resilient and redundant.
- **Security:** Sensitive information and critical assets that could cause widespread damage if compromised should be secured using best practices for data, network and systems protection. ICT security includes the prevention, protection and restoration of computers, services and communications, including the data and information contained therein, from risks or threats to their confidentiality, integrity and availability.
    - Confidentiality refers to the ability of an organization to ensure data is kept private and controlled to prevent unauthorized access.
    - Integrity refers to the ability of an organization to ensure data is trustworthy, accurate and reliable, including being free from tampering or manipulation.
    - Availability refers to the ability of an organization to ensure data is accessible to those who need it, and that technologies enabling that accessibility are functioning as they should and when needed.

The ICT function ensures that incident response staff have secure access to their agency networks and systems, including the ability to query, modify and/or add updated information, and securely share data. The proliferation of portable and mobile devices that support voice, data and video communications drives the demand for on-scene access to sensitive information. This results in an increased need to develop secure technology and procedures to protect personal identifiable information (PII) and other sensitive information from cybersecurity risks, threats and vulnerabilities. During an incident that affects the cybersecurity integrity of the response operation, the incident commander may designate the ICT function to support and oversee the responding organizations and responders' requirements for IT systems and network access; however, the ICT Branch is not directly responsible for responding to a cyber incident.

2. Impact of Hazards on ICT Capabilities

Threats to ICT operations may be natural, adversarial or human-caused, or technological. Table 1 describes each hazard and its potential impact on ICT operations.

Table 1: ICT Impacts by Type of Hazards

Type of Hazards	Impact
Natural Hazard	These events are emergencies caused by forces of nature such as storms, earthquakes and other natural events. Natural hazards can impact access to communications capabilities and IT resources. While many of these natural hazards are more likely to affect fixed critical infrastructure, they can also affect temporary resources. A natural hazard that significantly damages fixed infrastructure can have cascading effects. For example, a major earthquake can break buried fiber optic lines critical to accessing IT networks or reaching an emergency call center.
Adversarial or Human-Caused	These are disasters created by man, either intentionally or by accident. Human-caused acts can disrupt or alter voice, data, or video communications by intercepting traffic, altering records and information, or forcibly encrypting content in a manner that prevents access, such as during a ransomware attack. Accidental acts can include operator errors that may shut off key components to a network or overloading a network to create an unintended denial-of-service condition. Additional examples include hardware failure and bugs in the software.
Technological	These incidents involve materials and tools created by man and that pose a unique hazard or vulnerability to the general public and environment. The jurisdiction needs to consider incidents that are caused by accident (e.g., mechanical failure, human mistake), result from an emergency caused by another hazard (e.g., flood, storm), or are caused intentionally.

ICT Branch Organization, Roles and Responsibilities

The requirements to establish and manage the potential scope of ICT functions to support today's incidents have become increasingly complex. The ICT Branch provides a structure with the flexibility to expand and contract to support the full scope of the ICT requirements as needed.

NIMS Command and Coordination

The NIMS Command and Coordination component describes the systems, principles and structures that provide a standard national framework for incident management.

ICT capabilities are central to every level of an incident, regardless of its size or scope. The actual ICT structure may change in size to meet the complexity needs of incident management.

1. Span of Control

The ICS organizational structure can be scaled to incorporate additional elements based on the incident's type, size, scope and complexity. 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 Incident Commander only fills the positions required to support the incident objectives. The flexibility of this guidance allows the Incident Commander or Unified Command to appoint an ICT Branch Director or assign the Logistics Section Chief to manage the ICT Function.

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 a Communications Unit, IT Service Unit and/or Cybersecurity Unit. The Communications Unit manages the planning and implementation of interoperable radio services. The IT Service Unit manages data and IT planning and implementation. The Cybersecurity Unit identifies cybersecurity vulnerabilities, assesses threats to the ICT infrastructure and the incident management organization and recommends risk mitigation actions.

2. The ICT Branch

The ICT Branch consolidates ICT services within one branch in the Logistics Section while designating the delivery of services as either interoperable communications, IT or cybersecurity services. This organization streamlines incident communications and IT requirements within the Logistics Section. There are potentially three units within the ICT Branch:

- **Communications Unit:** Oversees the delivery of interoperable communications, including the management of radio and telephone equipment.
- **IT Service Unit:** Delivers data services, including by managing the Unified Help Desk and securing data network systems.
- **Cybersecurity Unit:** Identifies cybersecurity risks and vulnerabilities and assesses threats to the ICT infrastructure and the incident management organization.

Figure 1 shows an example organization chart of the ICT Branch.

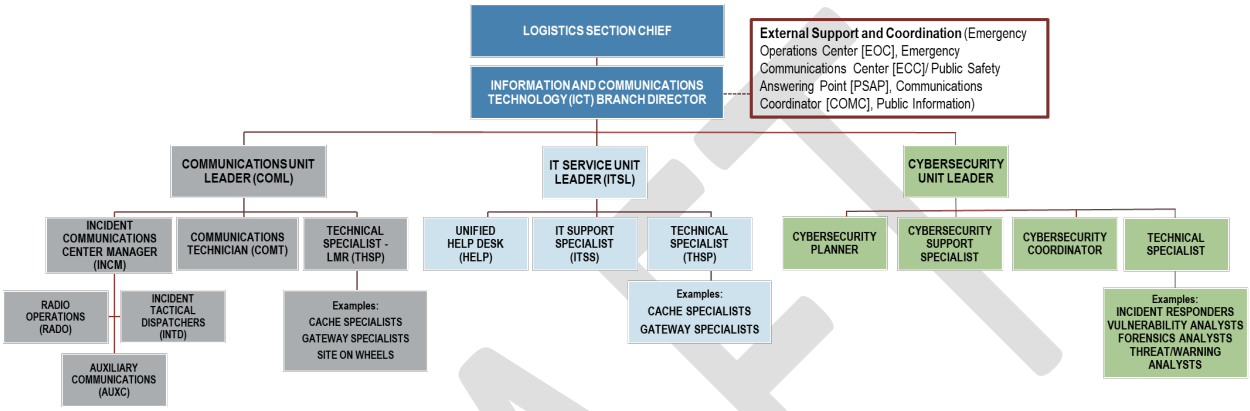

Figure 1: Example ICT Branch Organizational Chart

The ICT Branch frequently coordinates with:

- **Incident Command or Unified Command**, which may provide overarching direction and incident objectives during an incident.
- **Public Information**, which requires alerts and warning, website, social media and TV/radio broadcast functionality supported by ICT infrastructure.
- **Operations Section**, which provides tactical direction during an incident. During a cybersecurity incident, there may be significant coordination between operational cybersecurity functions and the ICT Branch.
- **Planning Section**, which requires geospatial and other information-sharing services supported by the ICT infrastructure.
- **Emergency Operations Center (EOC)**, which may have staff directing operations or providing support for IT and telecommunications services. If the EOC utilizes the Emergency Support Function (ESF) construct, these activities may reside in the EOC's ESF #2 – Communications function. ESF #2 is just one possible location for these communications support and telecommunications restoration and recovery activities, as it is possible the EOC may leverage additional unique Emergency Support Functions for IT or cybersecurity activities or a departmental or ICS-like structure to house these IT and telecommunications functions.
- **Emergency Communications Center (ECC)/Public Safety Answering Point (PSAP)**, which may provide additional communications support to the ICT Branch, dispatching and radio operator

services and provide 24/7 monitoring and troubleshooting of communications systems and networks.

- **Communications Coordinator (COMC)**, who provides coordination and deconfliction of spectrum resources and other communications capabilities between multiple incidents. The COMC serves as a point of contact (POC) and is responsible for maintaining contact with local agencies, collecting information about local resources to aid the COML and helping with tasks such as ordering and assigning equipment and frequencies and tracking the status of orders.

3. Leadership

3.1. Logistics Section Chief

The Logistics Section Chief leads the Logistics Section, including the ICT Branch. When an incident requires several facilities and/or large quantities of equipment, the Logistics Section Chief may establish branches, such as the ICT Branch. This helps maintain a manageable span of control to provide more effective supervision and coordination among the units. The Logistics Section Chief has authority over the ICT Branch Director.

3.2. ICT Branch Director

The ICT Branch Director establishes and manages the infrastructure and systems that support the incident's communication and information management needs. The ICT Branch Director should understand the dynamics of the ICT Branch and the technical requirements of establishing, maintaining and securing integrated communications for the incident, as well as providing recovery and/or continuity support should systems fail. The ICT Branch Director de-conflicts and prioritizes the allocation of ICT resources toward competing voice and/or data-centric uses. The ICT Branch Director manages all aspects of the ICT function and builds the branch downward, as required, to maintain a manageable span of control. The ICT Branch Director prioritizes and mitigates risks to ICT infrastructure originating from known or suspected threats or vulnerabilities.

4. Personnel

The ICT Branch should have personnel with knowledge of radio frequency operations, cybersecurity planning skills, familiarity with network operations, an understanding of software and hardware, and insights into voice, data and video systems. Staff should also be able to troubleshoot network access challenges and solve faulty operation problems.

If organizations do not have staff with this expertise, they may identify private sector subject-matter experts who can mobilize to incidents when needed. ICT Branch staff may support multiple incidents if the incidents are small and require few resources. For these situations, the ICT Branch may leverage support from remote staff.

Though the ICT Branch secures technology and access to agency networks, all personnel assigned to an incident authorized to use connected technology to perform their duties are responsible for abiding by security protocols and mitigating against potential cybersecurity breaches.

5. Communications Unit

The Communications Unit is responsible for all incident radio communications, including for:

- Documenting all radio channel resource assignments;
- Assigning voice radio channels;
- Producing the Incident Radio Communications Plan (ICS 205) for the most complex incidents;
- Establishing voice networks for command, tactical, support and air units;
- Setting up on-scene telephony;
- Providing any necessary off-incident communications links;
- Installing and testing communications equipment;
- Supervising and operating the incident communications center;
- Distributing and recovering communications equipment assigned to incident personnel;
- Maintaining and repairing communications equipment onsite; and
- Maintaining coordination with information and communications technology service providers.

Table 2 lists key roles in the Communications Unit and their responsibilities. Appendix C lists additional details about the roles and responsibilities in the Communications Unit.

267 **Table 2: Communications Unit Roles and Responsibilities**

Role	Responsibilities
Communications Unit Leader (COML)	▪ Plans and manages the technical and operational aspects of meeting the communications needs of an incident or event ▪ Supervises unit personnel and is responsible for performance of subordinate position duties that are not filled or delegated ▪ Participates in incident action planning meetings ▪ Prepares the Incident Radio Communications Plan (ICS Form 205) ▪ Establishes and supports communication capabilities ▪ Establishes an Incident Communications Center (ICC) ▪ Requests communications personnel, equipment, supplies and services ▪ Coordinates with Information Technology Service Unit Leader (ITSL) to maintain systems capabilities and performance
Incident Communications Center Manager (INCM)	▪ Manages an ICC ▪ Supervises Incident Tactical Dispatcher (INTD) and Radio Operator (RADO) positions in the ICC ▪ Provides support and assistance to the COML
Incident Tactical Dispatcher (INTD)	▪ Operates in an ICC and leverages their multi-tasking, communication, accountability and documentation skills of successful telecommunicators to provide public safety communications expertise and support at planned events and extended incidents ▪ Manages for all radio traffic, telephone call processing, data communications and various forms of documentation tasked to the ICC ▪ Supports the ICC as a single resource or as part of an incident tactical dispatch team
Radio Operator (RADO)	▪ Manages radio traffic, telephone call processing, data communications and various forms of documentation tasked to the ICC

Role	Responsibilities
Incident Communications Technician (COMT)	▪ Provides guidance and support to the COML in developing the Communications Plan ▪ Assesses and determines radio system coverage requirements or capabilities ▪ Installs, tests and troubleshoots communications equipment and systems ▪ Programs or verifies programming of radio equipment ▪ Maintains and repairs equipment ▪ Manages cache equipment, batteries and gateways ▪ Distributes and tracks equipment ▪ Resolves interference issues ▪ Trains users on equipment
Auxiliary Communicator (AUXC)	▪ Installs appropriate/approved Auxiliary Communications equipment per discussion with the COML or INCM ▪ Tests all components of Auxiliary Communications equipment to ensure systems are operational ▪ Establishes Auxiliary Communications area(s) of operation ▪ Interacts and coordinates with appropriate Auxiliary Communications operational personnel

6. Information Technology Service Unit

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 during duration of incident; and
- Coordinating on passwords and security access as directed during the duration of the incident.

282 Table 3 lists key roles in the IT Service Unit and their responsibilities. Appendix C lists additional
283 details about roles and responsibilities in the IT Service Unit.

284 **Table 3 : IT Service Unit Roles and Responsibilities**

Role	Responsibilities
Information Technology Service Unit Leader (ITSL)	▪ Plans and manages the technical and operational aspects of meeting the data and application needs of an incident or event ▪ Supervises unit personnel ▪ Performs subordinate positions duties that are not filled or delegated ▪ Participates in incident action planning meetings ▪ Prepares the Information Technology Plan ▪ Establishes and supports on-scene IT infrastructure and application capabilities ▪ Establishes the Unified Help Desk ▪ Coordinates support with the IT Departments of all responding agencies ▪ Orders or requests personnel, supplies and equipment
Incident Technology Support Specialist (ITSS)	▪ Establishes and maintains networks sufficient to support incident needs ▪ Installs and configures IT hardware and software components ▪ Responds to work tickets generated by the Unified Help Desk ▪ Identifies, assesses and mitigates cybersecurity threats and vulnerabilities ▪ Performs daily IT support functions to include connectivity checks, software upgrades, system backups and server functions ▪ Troubleshoots system and equipment errors and connectivity problems and resolves most problems ▪ Provides initial computer and associated training including instructions on logging on and accessing network services

Role	Responsibilities
Unified Help Desk Manager (HELP)	▪ Establishes a Unified Help Desk function ▪ Uses an established process for receiving and tracking Work Order tickets ▪ Uses system established by the ICT Branch Director, ITSL and/or COML to prioritize, route or escalate Help Desk work tickets to proper tier or technical specialist (THSP) for analysis and resolution ▪ Assists the ITSL with forms and documentation

7. Cybersecurity Unit

The Cybersecurity Unit identifies cybersecurity vulnerabilities, assesses threats to the ICT infrastructure and the incident management organization and recommends 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 the responding organizations;
- Managing documentation and ensuring sensitive security information is properly controlled (e.g., PII, protected health information [PHI] and protected critical infrastructure information [PCII]);
- Performing system administration on specialized cyber defense applications and systems or virtual devices; and
- Assisting in identifying, prioritizing and implementing technical infrastructure and key resources utilized in cyber defense efforts.

Table 4 lists key roles in the Cybersecurity Unit and their responsibilities. Appendix C lists additional details about roles and responsibilities in the Cybersecurity Unit.

306 **Table 4: Cybersecurity Unit Roles and Responsibilities**

Role	Responsibilities
Cybersecurity Unit Leader	▪ Plans and manages the technical and operational aspects of meeting the cybersecurity needs of an incident or event ▪ Supervises unit personnel and is responsible for performance of subordinate positions duties that are not filled or delegated ▪ Participates in incident action planning meetings ▪ Develops and publishes a basic cybersecurity plan ▪ Establishes and supports on-scene cyber defense and application capabilities ▪ Coordinates support with the cybersecurity departments of all responding agencies ▪ Orders or requests personnel, supplies and equipment ▪ Documents and escalates incidents that may cause ongoing and immediate impact to the environment
Cybersecurity Planner	▪ Assesses planning needs and collaborates with stakeholders to develop cybersecurity related policies, plans, practices and guidelines for implementation ▪ Analyzes organization's cyber defense policies ▪ Configurations and evaluates compliance with regulations and organizational directives ▪ Integrates applicable laws, statutes and regulatory documents into policies, plans, practices and guidelines ▪ Promotes awareness of cybersecurity plans and strategies, as appropriate, among command and other stakeholders ▪ Monitors the implementation of cybersecurity policies, principles, practices and guidelines in the planning process ▪ Provides guidance and support to command during the development of cyber-related plans and policies ▪ Communicates threat and risk reports to Incident Command ▪ Develops strategies and plans for mitigating identified vulnerabilities and threats ▪ Develops security monitoring plan to detect potential malicious or suspicious activity that could impact response activities ▪ Assists ITSL with preparing the Information Technology Plan

Role	Responsibilities
Cybersecurity Coordinator	▪ Coordinates the development, promotion and sharing of cybersecurity information both within and outside the ICT Branch and the responding organizations ▪ Coordinates the integration of competing requirements and priorities from multiple agencies and internal/external stakeholders ▪ Identifies gaps and impediments across internal and external partner organizations or third-party services ▪ Coordinates with technical and operational staff to ensure the implementation and updating of specialized cyber defense applications based upon identified threats and vulnerabilities ▪ Coordinates with public information officers (PIO) for social media monitoring inputs ▪ Liaises with supporting IT and cybersecurity organizations, including vendors, volunteers, insurance companies and other outside partners ▪ Manages documentation and ensures sensitive security information is properly controlled, (e.g., PII, PHI and PCII)
Cybersecurity Support Specialist	▪ Performs system administration on specialized cyber defense applications and systems or virtual devices ▪ Assists in identifying, prioritizing and implementing technical infrastructure and key resources utilized in cyber defense efforts ▪ Builds, installs, configures and tests dedicated cyber defense hardware and services ▪ Assists in assessing the operational impact of implementing and sustaining cyber defense infrastructure ▪ Assesses and evaluates applications, hardware infrastructure, prevention and detection tools, access controls, and configurations of platforms managed by service providers ▪ Implements security monitoring plan

307

Appendix A: Acronym List

AUXC	Auxiliary Communicator
CDP	Center for Domestic Preparedness
CISA	Cybersecurity and Infrastructure Security Agency
COMC	Communications Coordinator
COML	Communications Unit Leader
COMT	Communications Technician
ECC	Emergency Communications Center
EOC	Emergency Operations Center
EMI	Emergency Management Institute
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
GIS	Geographic Information Systems
HELP	Incident Unified Help Desk
ICC	Incident Communications Center
ICS	Incident Command System
ICT	Information and Communications Technology
ICTAP	Interoperable Communications Technical Assistance Program
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatchers
IT	Information Technology
ITSL	Information Technology Service Unit Leader
ITSS	Information Technology Support Specialist

NIC	National Integration Center
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NTED	National Training and Education Division
POC	Point of Contact
PSAP	Public Safety Answering Point
RADO	Radio Operations
SLTT	State, Local, Tribal and Territorial
SOP	Standard Operating Procedure
THSP	Technical Specialist

Appendix B: Glossary

Branch: The Incident Command System (ICS) organizational level having functional or geographical responsibility for major aspects of incident operations. A branch falls between the Section Chief and the division or group in the Operations Section, and between the section and units in the Logistics Section. Branches are identified by Roman numerals or by functional area.

Communications Unit: Unit within the ICT Branch that oversees the delivery of interoperable communications, including by managing radio and telephone equipment.

Emergency Communications Center (ECC): The virtual or physical location that assists the public by receiving and processing 9-1-1 emergency calls and non-emergency calls; dispatching police, fire and emergency medical service units in an efficient, coordinated and professional manner.

Emergency Operations Center (EOC): The virtual or physical location where the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction.

Incident Command: The ICS organizational element responsible for overall management of the incident and consisting of the Incident Commander or Unified Command and any additional Command Staff activated.

Incident Command System (ICS): A standardized approach to the command, control and coordination of on-scene incident management, providing a common hierarchy within which personnel from multiple organizations can be effective. ICS is the combination of procedures, personnel, facilities, equipment and communications operating within a common organizational structure, designed to aid in the management of on-scene resources during incidents. It is used for all kinds of incidents and is applicable to small, as well as large and complex, incidents, including planned events.

Incident Communications Center (ICC): A facility or defined area activated to provide communications/dispatch support specifically dedicated to an incident or event.

Incident Support Model: An organizational structure where jurisdictions/organizations that focus their EOC team's efforts on information, planning and resource support map choose to separate the situation awareness function from planning and combine operations and logistics functions into an incident support structure. In an ISM EOC, situation awareness/information management reports directly to the EOC director and resource sourcing, ordering and tracking is streamlined.

Information Communications Technology (ICT): The capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer and interchange of data and information. ICT is broadly used to address the evolution and convergence of traditional telephone and radio with information technology (IT) systems.

Information and Communication Technology (ICT) Branch: ICS Branch responsible for performing ICT Function.

Information and Communications Technology (ICT) Function: Scalable and flexible NIMS component responsible for establishing, maintaining and securing integrated communications for the incident management organization.

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Information Technology Service Unit: Unit within the ICT Branch that delivers data services, including by managing the Unified Help Desk and securing data network systems.

Logistics Section: The ICS Section responsible for providing facilities, services and material support for the incident.

National Incident Management System (NIMS): A systematic, proactive approach to guide all levels of government, nongovernmental organizations and the private sector to work together to prevent, protect against, mitigate, respond to and recover from the effects of incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems and processes to successfully deliver the capabilities described in the National Preparedness System. NIMS provides a consistent foundation for dealing with all incidents, ranging from daily occurrences to incidents requiring a coordinated Federal response.

Public Safety Answering Point (PSAP): A call center designated to receive 9-1-1 calls and route them to emergency service personnel.

Section: The ICS organizational element having responsibility for a major functional area of incident management (e.g., Operations, Planning, Logistics and Finance/Administration).

Span of Control: The number of subordinates for which a supervisor is responsible, usually expressed as the ratio of supervisors to individuals.

Unit: The organizational element with functional responsibility for a specific activity within the Planning, Logistics and Finance/Administration Sections in ICS.

Unit Leader: The individual in charge of a unit in ICS.

Appendix C: Resources

1. Positions

FEMA, NIMS 509-12: Communications Coordinator (COMC), *pending publication*: Coordinates communications resources across multiple incidents.

FEMA, NIMS 509-12: Incident Communications Technician (COMT): Implements and maintains the communications infrastructure and radios. https://www.fema.gov/sites/default/files/2020-05/fema_nims_509_commstechnician_final_2.pdf

FEMA, NIMS 509-12: Communications Unit Leader (COML): Leads the Communications Unit. https://www.fema.gov/sites/default/files/2020-05/fema_nqs_ptb_commsunitld_finaln_0.pdf

FEMA, NIMS 509-12: ICT Branch Director, *pending publication*: Establishes and manages the infrastructure and systems that support the incident's communication and information management needs.

FEMA, NIMS 509-12: Incident Communications Center Manager (INCM), *pending publication*: Manages the Incident Communications Center.

FEMA, NIMS 509-12: Information Technology Service Unit Leader (ITSL), *pending publication*: Manages the personnel and operational needs of the IT Service Unit.

FEMA, NIMS 509-12: Incident Technology Support Specialist (ITSS), *pending publication*: Establishes and maintains networks sufficient to support incident needs.

FEMA, NIMS 509-12: Radio Operators (RADO), *pending publication*: Staffs the Incident Communications Center.

FEMA, NIMS 509-12: Incident Tactical Dispatchers (INTD), *pending publication*: Staffs the Incident Communications Center.

FEMA, NIMS 509-12: Unified Help Desk Manager (HELP), *pending publication*: Manages the Unified Help Desk function.

FEMA, NIMS 509-12: Auxiliary Communicator (AUXC), *pending publication:* Establishes and manages the Auxiliary Communications area of operations.

FEMA, NIMS 509-12: Cybersecurity Unit Leader, *pending publication:* Plans and managers the technical and operational aspects of meeting the cybersecurity needs of an incident or event.

FEMA, NIMS 509-12: Cybersecurity Planner, *pending publication:* Identifies cybersecurity vulnerabilities and assesses threats to the ICT infrastructure and the incident management organization.

FEMA, NIMS 509-12: Cybersecurity Coordinator, *pending publication:* Coordinates with cyber defense analysts to manage and administer the updating of rules and signatures for specialized cyber defense applications.

FEMA, NIMS 509-12: Cybersecurity Support Specialist, *pending publication:* Assists in identifying, prioritizing and coordinating the protection of critical cyber defense infrastructure and key resources.

2. Education and Training

2.1. Federal Emergency Management Agency (FEMA)

FEMA: The National Preparedness Online Course Catalog provides searchable, integrated information on courses provided or managed by FEMA's Center for Domestic Preparedness (CDP), Emergency Management Institute (EMI) and National Training and Education Division (NTED). To view the catalog, visit https://training.fema.gov/.

2.2. Cybersecurity and Infrastructure Security Agency (CISA)

CISA's Interoperable Communications Technical Assistance Program (ICTAP) serves all 56 states and territories. The Agency provides direct support to state, local, tribal and territorial (SLTT) emergency responders and government officials through the development and delivery of training, tools and onsite assistance to advance public safety interoperable communications capabilities.

CISA provides an Emergency Communications Technical Assistance Planning Guide of service offerings. The guide features new and updated offerings to support training and exercises, planning for broadband, radio re-programming for narrow banding, workshops for dispatch and mobile communications vehicles operations and more. To view the guide, visit https://www.cisa.gov/safecom/ictapscip-resources.