National Incident Management System

Emergency Operations Center How-to Quick Reference Guide

October 2022

FEMA

This page intentionally left blank

Table of Contents

Introduction 1

1. Purpose 1

1.1. NIMS Compliance and Integration 1

What is an Emergency Operations Center? 2

1. Hallmarks of an EOC 3

Preliminary Assessments 4

1. Hazard and Vulnerability Assessment 4

2. Capability Assessment 4

2.1. Interagency Coordination 5

2.2. Multiagency Coordination Groups 6

2.3. Private Sector 8

2.4. EOC Staffing Requirements and Structure Type 9

2.4.1. ICS OR ICS-LIKE STRUCTURE 10

2.4.2. Incident Support Model 11

2.4.3. DEPARTMENTAL STRUCTURE 11

2.4.4. ORGANIZATIONAL CONCEPT AND FRAMEWORK 11

2.4.5. EOC SKILLSETS AND USER GUIDE 12

2.5. EOC Facility Support 12

2.6. Plans and Procedures 13

2.7. Communications 13

2.8. Lifelines 14

Site Selection 15

1. General Considerations 15

1.1. Vulnerability 15

1.1.1. Central Location and Proximity to Key Personnel 16

1.2. Traffic Flow and Congestion 16

1.3. Accessibility 17

1.4. Parking 17

1.5. Communications 17
1.6. Security 18
1.7. Scalability 18
1.8. Community-Based Design 19
1.9. Alternate Sites 19
1.10. Existing EOC Sites 20
2. Mitigation Considerations 20
2.1. Natural Hazards 20
2.2. Technological and Human-Caused Hazards 20
2.3. Virtual and Hybrid Operations 20
EOC Capabilities and Requirements 21
1. Determining Personnel Space Requirements 21
1.1. EOC Functions 21
1.2. Space Requirements 21
1.3. Additional Personnel Space Requirements 22
1.4. Sustained Operations 22
2. Communications Requirements 22
2.1. Interoperability 23
2.2. Telecommunications (Including Teleconferencing, Videoconferencing, Text Messaging and Fax) 23
2.3. Public Safety Radio 24
3. IT Requirements 24
3.1. Internet Connectivity 24
3.2. Computer Systems 25
3.3. Audiovisual Support 26
4. Supplies and Equipment Requirements 26
4.1. Furniture and Office Equipment 26
4.2. Food Supply 26
4.3. Medical and Sanitary Supplies 27
4.4. Status and Situation Boards 27

4.5. Administrative Supplies 27
4.6. Support Services 27

Room Design Features 29
1. Design Considerations 29
1.1. Basic Room Designs 29
1.2. Emergency Power 31
1.3. Uninterruptible Power Supply 31
1.4. Physical Access 32
2. Considerations for Multiuse Facilities 32
2.1. Ancillary Space and Storage Areas 32
2.2. Operations Room 33
2.3. Classroom and Training Areas 33
2.4. Meeting Rooms 33
3. Floor Plans 33

Information Management Systems 34
1.1. Information/Data Management Tools 34
1.2. Geospatial Data and Analysis Capability 34
1.3. Crowdsourcing in Emergency Management 35
1.4. Hazard Prediction and Monitoring Capability 36
1.5. Crisis Information Management System 36
1.6. Personnel Qualification and Certification System 37
2. Infrastructure for Communications and Data Management 37
2.1. Adequate Numbers of Phones, Multifunction Copy/Scan/Print/Fax Devices, Copiers, Computers 37
2.2. Secure Communications 38
3. Cybersecurity 38

EOC Management 40
1. Standard Operating Procedures 40
1.1. Authority 40

1.2. Elected Officials, Senior Leaders, and Tribal Representatives 40
1.3. Conditions for Activation 41
1.4. Notice Events 41
1.5. Notifications 42
1.6. Setup 42
1.7. Deactivation 43
1.8. Annual Review 43
1.9. Testing and Exercising Activation Procedures 43

Planning, Training and Exercises 44

1. Planning 44
1.1. The Preparedness Cycle 44
1.2. Incident Action Planning 45
2. NIMS Training and EOCs 46
2.1. EOC Training Progression 46
3. Exercises and EOCs 48
3.1. HSEEP Principles 48
3.2. Exercise Types 49
3.3. Equipment Checks 50
3.4. Evaluation and Improvement 50

Resource Management During an Incident 51

1.1. Identifying Requirements 51
2. Ordering and Acquiring 52
2.1. Resource Requests 52
2.2. Incident Assignments 53

Abbreviations 54

Glossary 58

References and Resources 73

COVID-19 Pandemic Operational Guidance 73

Cybersecurity *73*
Emergency Support Function (ESF) *73*
FEMA National Training and Education Division (NTED) *73*
Incident Command System (ICS) Resource Center *74*
Incident Action Planning Guidance *74*
Lifelines *74*
National Incident Management System (NIMS) *74*
National Qualification System (NQS) *74*
NIMS Training Program *75*
NQS EOC Skillsets and EOC Skillsets User Guide *75*
OneResponder *75*
Threat and Hazard Identification and Risk Assessment (THIRA) *75*
Vulnerability Assessment *75*

Annex **76**

1. Emergency Operation Center (EOC) Self-Assessment Tool **76**

2. Tips for Using This Tool **76**

3. More Information **77**

4. Facility Features **78**

5. Survivability **80**

6. Security **81**

6.1. Facility 81

6.2. Communications/Networks 81

6.3. Personnel 82

7. Sustainability **83**

7.1. Facility 83

7.2. Communications/Networks 83

8. Interoperability **85**

8.1. Communications 85

8.1.1. REQUIREMENTS 85

8.1.2. RADIOS 85

8.2. Procedures 86

8.3. Training 86

9. Flexibility **87**

9.1. Facility 87
9.1.1. PRIMARY EOC 87
9.1.2. ALTERNATE EOC 87
9.2. Communications/Networks 88
10. Other Considerations 90
Geographic data and analysis capability *90*
Hazard prediction and monitoring capability *90*
Crisis information management system *90*
Personnel qualification and certification system *90*
11. Additional Comments and Other Key Information 91

Introduction

The routine, day-to-day management of government differs greatly from emergency operations. During an emergency, effective decision-making relies on leaders' ability to collect emergency-related information, which requires close coordination between key officials from a variety of departments, agencies and organizations.

Having a coordination structure such as an Emergency Operations Center (EOC), from which leaders can coordinate and direct emergency efforts, is essential for emergency response and recovery.[1] Governments, jurisdictions, municipalities, nongovernmental organizations (NGO) and members of the private sector, at all levels, should prepare for the possibility of an emergency that will significantly change operating procedures. Governments must be ready to direct and control emergency operations.[2]

1. Purpose

The purpose of this all-hazards how-to guide is to provide state, local, tribal and territorial (SLTT) jurisdictions with information and guidance related to setting up, operating, maintaining and deactivating an EOC that successfully meets the jurisdiction's needs. This guidance applies an all-hazards approach in its concepts, processes and principles. The Federal Emergency Management Agency (FEMA) recognizes that certain hazards (such as COVID-19) may have specific implications, precautions and instructions that take effect under certain conditions and threat environments.

1.1. NIMS Compliance and Integration

Leaders should consider the National Incident Management System (NIMS) framework and principles when developing an EOC. Using appropriate terminology is especially important for ensuring consistency among jurisdictions at all levels of government.

[1] An exception to the need for a central location could be when planning for a pandemic, in which case leaders should consider telecommuting or other policies that impose physical distance.

[2] References to non-federal products throughout this document are provided as examples and not intended as an endorsement of any non-federal products by FEMA, the Department of Homeland Security (DHS) or the federal government.

What is an Emergency Operations Center?

An EOC is a central command and control system responsible for carrying out the principles of emergency preparedness and emergency management, or disaster management at a strategic level during an emergency, and ensuring the continuity of operation of a company, political subdivision, or other organization. An EOC is a location from which leaders of a jurisdiction or organization coordinate information and resources to support incident management activities (on-scene operations). EOC team structure and composition can vary widely. Virtual or hybrid EOCs may be used to expand the EOC when physical space is limited, to create a safer operating environment (e.g., for social distancing measures or if access to the EOC is impeded), to include additional stakeholders from the whole community who may not be able to be physically present or to support coordination during incidents in which conditions do not require in-person coordination to perform EOC functions.

An EOC is a physical, virtual or hybrid location and may be housed in a temporary facility or in a permanently established, central facility—perhaps a building that supports another government agency within the jurisdiction.

Deciding how to organize the EOC staff depends on factors such as the jurisdiction or organization's mission, authorities, staffing, partner/stakeholder agencies represented, EOC facilities, communications capabilities and engaged elected officials. For more information on EOC structures and organization methods, see the Capability Assessment section of this guide.

Jurisdictions establish EOCs to meet their unique requirements and needs, so no two EOCs have exactly the same design. Some jurisdictions see the EOC as the nerve center and tactical hub for incident response. Others see an EOC as a resource coordination center that locates and deploys resources but does not direct tactical-level responses. Some envision an EOC as a room with stadium seating and rows of desks facing large screens, while others imagine an open room with tables and chairs for each Emergency Support Function (ESF). In the end, the structure and functions largely depend on the requirements of the individual jurisdiction.

Primary functions of staff in EOCs, whether virtual or physical, include:

- Collecting, analyzing and sharing information;
- Supporting resource needs and requests, including allocation and tracking;
- Coordinating plans and determining current and future needs; and
- In some cases, providing coordination and policy direction.

1. Hallmarks of an EOC

An EOC is a coordination structure for collecting, analyzing and sharing information. During an incident, the EOC collects a large amount of data from multiple sources. Analysts from appropriate stakeholder organizations analyze the data and distill it into reports so that decision makers have the best possible information and intelligence when deciding how the jurisdiction will respond. Further, the EOC communicates information to response team members in the field, giving them greater insight into their work.

All EOCs have the following three hallmarks:

- An EOC supports resource needs and requests, including allocation and tracking.
    - An EOC serves as a single source for requesting additional resources from across the jurisdiction and from surrounding jurisdictions. Whether the EOC gives tactical instructions or dispatches resources requested from tactical commanders depends on the jurisdiction. However, all EOCs can analyze data, identify shortfalls, find resources, dispatch resources and monitor their return in order to give personnel on the ground the support they need to do their job.
- An EOC coordinates plans and determines current and future needs.
    - An EOC is a synthesis of multiple departments, agencies and organizations that work together in a coordinated fashion. EOC personnel facilitate a standard planning process to achieve EOC objectives. They also provide a range of planning services to address current needs and anticipate and devise ways to meet future needs.
- An EOC provides coordination and policy direction.
    - An EOC helps to integrate stakeholders and works with senior officials to facilitate the development of policy direction for incident support. EOC personnel work with legal counsel, authorize relevant protocols and procedures for response and coordination, and ensure the dissemination of timely, accurate and accessible information to the public. In addition, the staff in an EOC liaise with other government agencies at all levels, including federal and SLTT.

Preliminary Assessments

Before establishing an EOC, jurisdictions conduct hazard and vulnerability assessments and capability assessments to ensure that the facility can withstand the impacts of potential hazards and can implement a coordinated response to these hazards. If using a hybrid or virtual environment, hazard and vulnerability assessments may include additional facilities, including the homes and offices of staff members and key stakeholders. Other tools beyond these suggestions may exist, such as RAPT, that support visualizing and assessing challenges to community resilience.

1. Hazard and Vulnerability Assessment

Each jurisdiction conducts a hazard, vulnerability, and risk assessment to identify natural, technological and human-caused threats and hazards and rank them based on their likelihood and potential consequences. Jurisdictions use the assessment results to determine the EOC's physical design, ideal location and necessary capabilities. This work is essential because an EOC must be designed to withstand the impacts of likely hazards. FEMA's Threat and Hazard Identification and Risk Assessment (THIRA) provides detailed information that can be used for this process. In a hybrid or virtual environment, it is possible that alternate locations (including homes and offices of staff members and key stakeholders) may not be built to the same standards of a physical EOC.

Resilience Analysis and Planning Tool

FEMA designed the Resilience Analysis and Planning Tool (RAPT) to help emergency managers at local, state and regional levels visualize and assess challenges to community resilience.

RAPT allows users of all GIS skill levels to assess county-level challenges to resilience and to tell a visual story of priority needs for a range of issues, such as the following:

- Populations that may have greater challenges because of socioeconomic characteristics or proximity to critical infrastructure
- Potential difficulties in re-establishing community lifelines after a disaster
- Community zoning or land use plans that conflict with local hazards

2. Capability Assessment

The next step in planning an EOC is to identify the capabilities the EOC must have in order to coordinate a response to the identified hazards and risks. A capability assessment is a fundamental concept of emergency planning at all levels of government. The EOC capability assessment includes various considerations outlined in the following sections.

2.1. Interagency Coordination

Local authorities handle most incidents using communications systems, dispatch centers and incident personnel within a single jurisdiction. Larger and more complex incidents may begin with a single jurisdiction but rapidly expand to multi-jurisdictional and multidisciplinary efforts requiring outside resources and support.

EOC staff members coordinate with agencies/organizations inside and outside their jurisdiction that may provide assistance during an emergency. These include county, regional, state, and tribal stakeholders who have response and recovery roles and responsibilities, or who represent other entities (for example, port authorities, mass transit agencies, regional task forces and critical infrastructure owners and operators) and assist through formalized agreements. County EOCs typically coordinate directly with state EOCs. State EOCs function much like county EOCs, except they are also in direct coordination with federal agencies.

The Command and Coordination component of NIMS provides the user community with systems, principles and structures. Incident Command and Coordination consists of four areas of responsibility:

- **Tactical activities** to apply resources on scene;
- **Incident support**, typically conducted at EOCs:
    - Operational and strategic coordination
    - Resource acquisition
    - Information gathering, analysis and sharing;
- **Policy guidance** and senior-level decision-making; and
- **Outreach and communication** with the media and public to keep them informed about the incident.

Additional considerations for Information Technology in an EOC can include:

- Internal and external software licensing agreements and interoperability;
- File storage, access and security; and
- Agency policies around the use of specific ecosystems (e.g., Office 365, Google Workspace) or even proprietary systems when collaborating. This may also include collaboration with private sector partners, the use of external or guest accounts, and general permission levels associated with hybrid or virtual tools.

Additionally, hybrid or virtual EOC models allow for the expansion of an EOC beyond the bounds of typical space requirements. However, choosing a system that provides this scalability should balance access needs, including the ability to handle an increased user base, internal and external access concerns, and the user experience on virtual machines, desktops, laptops, tablets and phones.

Multiagency coordination and Unified Command requirements influence EOC design and space requirements. Leaders should consider several factors during the EOC design phase:

- During large incidents, outside agencies and organizations often send representatives to the EOC. These team members may need specialized communications equipment, power sources and parking for support vehicles.
- An EOC may need to expand as an incident becomes more complex. To avoid functionality issues, design the EOC to accommodate expanding on-site personnel numbers.
- The size of the jurisdiction's population may play a role in how large the facility should be.
- Jurisdiction size and population growth both play into interagency coordination, since agencies grow with the population.

2.2. Multiagency Coordination Groups

Multiagency Coordination Groups (MAC Groups), sometimes called Policy Groups, typically consist of agency administrators or organization executives or their designees. MAC Groups provide policy guidance to incident personnel, support resource prioritization and allocation, and enable decision-making among elected and appointed officials and senior executives—both those in other organizations and those directly responsible for incident management.

For more information on the organizational context of the NIMS Command and Coordination component, see Figure 1 and Figure 2 below, copied from FEMA training course E/G/L 0400: Advanced Incident Command System for Command and General Staff – Complex Incidents.

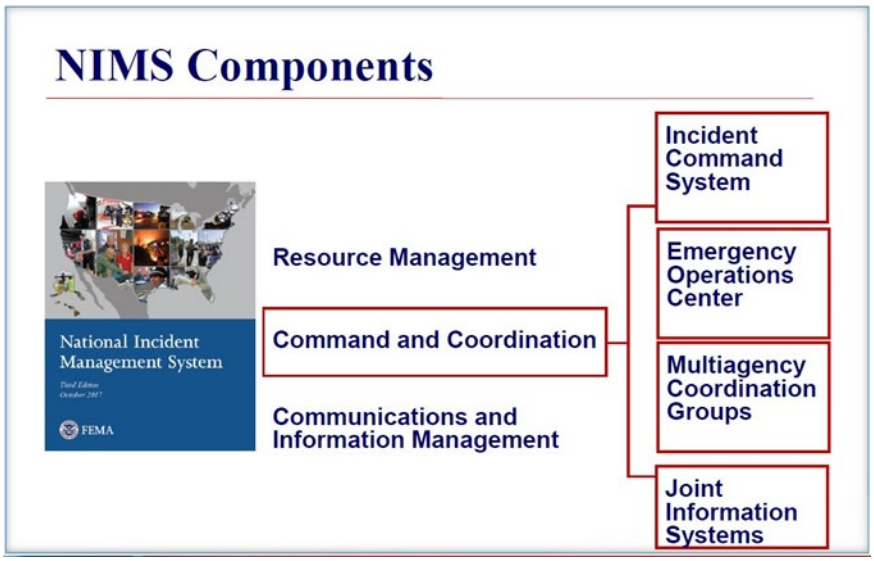

Figure 1. NIMS Components: Command and Coordination

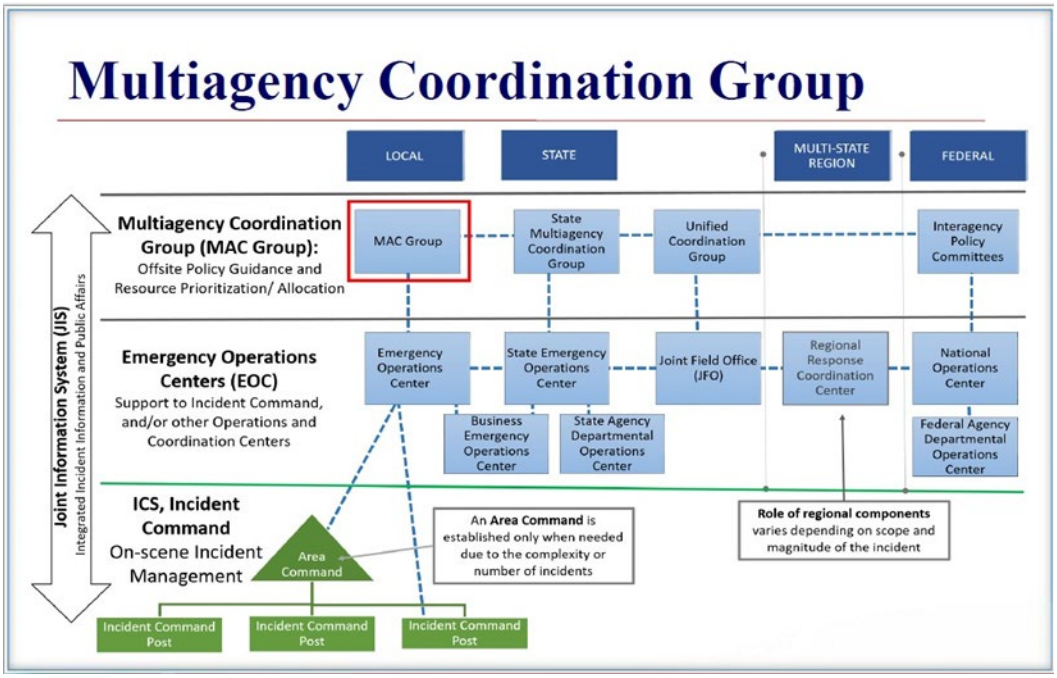

Figure 2. NIMS Components: Multiagency Coordination Group

Note: Do not confuse this type of interagency coordination with the NIMS Multiagency Coordination System (MACS). Under NIMS, MACS provides the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration and information coordination. MACS components include facilities, equipment, EOCs, specific multiagency coordination entities, personnel, procedures and communications. These systems help agencies and organizations fully integrate the subsystems of NIMS.

2.3. Private Sector

FEMA defines community resilience—a core capability under the mitigation mission area of the National Preparedness Goal (NPG)—as the capacity of individuals, communities, businesses, institutions and governments to adapt to changing conditions and to prepare for, withstand and rapidly recover from disruptions to everyday life, such as natural disasters and hazardous materials (HAZMAT) incidents. Community resilience grows through public-private relationships—by integrating shared capabilities and resources in planning, exercising and systematically incorporating key lessons learned across the whole community emergency management experience.

Private sector entities own and operate the majority of the nation's critical infrastructure. Private sector organizations therefore play a key role in providing goods, services, knowledge and technical expertise that can complement and ensure the effectiveness of the public sector's preparedness, response, recovery and mitigation operations. The private sector encompasses organizations and entities that are not part of any governmental structure. Private sector organizations include NGOs, trade associations, academia, businesses and industry. NGOs are also essential infrastructure partners in emergency planning, coordination, management and response.

Private sector organizations and NGOs are critical components in the effort to enhance the nation's resilience to natural and human-caused disasters. FEMA views the private sector as equal—and equally responsible—partners with the public sector in every phase of emergency management. Private sector and NGO partners provide value by engaging in a variety of activities:

- Participating in fusion centers and EOCs;
- Conducting joint training activities;
- Educating the public on emergency preparedness;
- Ensuring the efficient and effective use of available resources during an emergency;
- Developing and enhancing plans and protocols for emergency response, assessment, resource sharing, etc.;
- Developing and enhancing plans for integrating nongovernmental entities in preparedness, response and recovery; and
- Sharing critical information in preparation for and in response to an incident.

Private sector and NGO participation in emergency management planning and coordination provides EOCs with critical information on private sector and NGO issues, such as operational timelines, facility locations, building access needs, transportation needs, relocation logistics, security issues and recovery priorities.

Note: The National Business Emergency Operations Center (NBEOC) is FEMA's virtual clearinghouse for two-way information sharing between public and private sector/NGO stakeholders before, during

and after disasters. For information about the features, capabilities and requirements of virtual EOCs, see the Room Design Features section of this guide. To see the Business Emergency Operations Center (BEOC) Quick Start Guidance fact sheet, visit https://www.fema.gov/sites/default/files/2020-07/beoc-fact-sheet.pdf.

2.4. EOC Staffing Requirements and Structure Type

In planning for an EOC, leaders should factor in the types and numbers of personnel who will work in the facility to ensure its success—not only local personnel but other liaisons and representatives who may be present in the EOC during activations. Staffing should support sustained operations and provide the deepest roster that is feasible at each position. In other words, planners should consider the maximum staffing levels that may be necessary, along with what is practical for their jurisdiction.

A significant advantage of a hybrid or virtual environment is the ability to move between different EOC structure models based on the incident type, technology limitations, and staffing availability. Without the limitations of a physical space, virtual environments enable a "flattening" of the incident management system across field-based command structures, support-focused emergency operations centers and policy-level Multiagency Coordination Groups. The structure and flow of communication and coordination across all stakeholders are dynamic and evolving based on the needs of the incident(s).

The box below outlines various considerations for staffing and configuring an EOC.

Considerations for EOC Configuration and Staffing

EOC team configurations can vary widely based on the following considerations:

- Jurisdictional/organizational authorities;
- Available staffing and staff schedules;
- Partners and stakeholders represented;
- EOC facilities and capabilities;
- Engaged elected officials; and
- Nature and complexity of the incident or situation.

Like the ICS, the EOC structure follows the NIMS management principle of modular organization, which indicates that leaders are responsible for the functions of unstaffed subordinate positions.

Leaders should structure their EOC teams based on one of the common organizing methods that NIMS identifies (see Table 1). The explanations below can help leaders decide which EOC organizational structure best fits their situation, enabling them to respond most efficiently and effectively. Jurisdictions should consider which type best fits their needs.

Table 1: EOC Organizational Structure in NIMS

Structure Type	Benefits
ICS or ICS-like Structure	The ICS organizational structure is familiar to those with ICS training. It most closely aligns with the structure used for on-scene incident management.
Incident Support Model	This structure puts the EOC director in direct contact with those conducting situational awareness and information management. It streamlines resource sourcing, ordering and tracking.
Departmental Structure	By operating in the context of their normal relationships, department/agency representatives can function in the EOC with minimal preparation and startup time.

2.4.1. ICS OR ICS-LIKE STRUCTURE

Many jurisdictions use an ICS or ICS-like structure in their EOC. This is typically because emergency managers are familiar with the structure, and it aligns with the structure used in the field. It also provides a useful functional breakdown, particularly for EOCs that might take on operational missions. An ICS-like EOC structure generally reflects the standard ICS organization but with variations to emphasize the coordination and support mission of EOCs (as opposed to the tactical and logistics management role of on-scene responders). For example, EOC leaders often differentiate between field personnel and EOC personnel by adding "Support" or "Coordination" to EOC section titles. Additionally, some EOC leaders may modify certain ICS processes or functions to better reflect EOC activities and responsibilities.[3] EOC leaders may select a standard ICS organization for one or more of these reasons:

- EOC staff provide tactical direction to an incident;
- EOC management wishes to use ICS-trained personnel with no additional training requirements; and
- EOC managers want to mirror the organization of on-scene personnel.

[3] For more information about the ICS structure, see the NIMS document: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf.

2.4.2. INCIDENT SUPPORT MODEL

The Incident Support Model is a variation of the ICS structure. It does the following:

- Regroups the information management and situational awareness functions of the ICS Planning Section, and the intelligence dissemination function of the ICS Intelligence/Investigations Section, if necessary; and
- Combines the functions of the ICS Operations Section, the ICS Logistics Section and the comptroller/purchasing functions of the ICS Finance/Administration Section.

EOCs that use an Incident Support Model structure typically focus exclusively on support functions rather than on operations or managing response/recovery efforts. As with the ICS or ICS-like structure, the director of an Incident Support Model EOC has support personnel assigned to key functions, plus subject matter experts and technical specialists.

2.4.3. DEPARTMENTAL STRUCTURE

Jurisdictions and organizations may choose to maintain their relationships with the departments and agencies they already work with in responding to and recovering from incidents. Leaders can then configure their EOC staff by the team members' departments, agencies and organizations. Leaders can also organize by ESF rather than by department.

Staff in departmentally structured EOCs typically require less training than staff in other EOC structures. Departmentally-structured EOCs emphasize coordination and equal footing among all departments and agencies. In this model, a single individual—either the jurisdiction's emergency manager or another senior official—directly coordinates the jurisdiction's support agencies, NGOs and other partners. Departmental representatives bring the resources, expertise and relationships associated with their organizations and functions. The EOC makes decisions to achieve mutually agreed-upon objectives, as in a Unified Command. The roles and responsibilities of a departmental EOC reflect the day-to-day responsibilities of the represented departments and agencies. This structure enables jurisdictions and organizations to address incidents effectively while maintaining their normal authorities, responsibilities and relationships.

2.4.4. ORGANIZATIONAL CONCEPT AND FRAMEWORK

NIMS describes in detail the three organizational methods defined above. Recognizing the broader context of coordinating structures, NIMS gives leaders the flexibility to adopt other response structures used in various organizations. These methods, often used alongside other approaches, outline who responds in emergencies and how these coordinating partner organizations, functional units and others work together to respond to and recover from events. These EOC configuration options include the following:

- Major management activities method: This structure includes a focus on primary actions guided by management decisions. The Policy Group, coordination group, operations group and resources group are responsible for executing those decisions.

- ESF organizational method: This structure provides the flexibility to align and assign stakeholder resources according to their capabilities, tasks and requirements to augment and support the EOC's response. The ESF model also provides well-defined lines of communication between departments, local jurisdictions and federal agencies. Though many state and local jurisdictions follow the federal government ESF model, this model may not apply to smaller jurisdictions. For more information, visit https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response#esf.

2.4.5. EOC SKILLSETS AND USER GUIDE

The diversity among EOCs can create challenges in sharing personnel across jurisdictions' EOC organizations. Different EOCs may use different titles for positions performing similar functions or may assign different responsibilities to similarly titled positions. As part of the National Qualification System (NQS), EOC Skillsets support standardized qualifications for EOC personnel, while remaining flexible enough to accommodate individual EOCs of all sizes and kinds, regardless of organizational structure.

The EOC Skillsets describe common EOC functions and provide a flexible approach to qualifying EOC personnel. EOC leaders, representing any level of government or the private sector or NGOs, can mix and match skillsets, combining them to create EOC Position Task Books (PTBs) that reflect the EOC's personnel needs. PTBs identify the minimum competencies, behaviors and tasks that personnel demonstrate to become qualified for a defined incident management or support position.

The EOC Skillsets User Guide explains what EOC Skillsets are and how to use them to construct PTBs. The box below provides a real-world example of how an organization used EOC Skillsets to construct PTBs. To download the EOC Skillsets and EOC Skillsets User Guide, visit https://www.fema.gov/emergency-managers/nims/components/emergency-operations-center.

Real-World Use of EOC Skillsets:

New York State Division of Homeland Security & Emergency Services

"Last fall, members of NYS DHSES OEM completed the L2300 course. One of the biggest take-aways that we got from the class was a much clearer understanding of how to use the twenty NQS EOC Skillsets, along with NYS-developed skillsets, to develop comprehensive PTBs for our own state EOC positions. We presented a proposal to do that in OEM, our executives immediately saw the advantages, as it addressed qualifying and credentialing challenges in the state EOC, and in December 2019 we launched a Project Team to begin work on this."

— Chief of Headquarters and Incident Management Team Operations

2.5. EOC Facility Support

While the focus of EOC planning is to build the staffing capacity to coordinate response activities, planners must remember that the EOC is a facility and therefore requires facility management.

Examples of EOC facility support include security, parking, break rooms, IT infrastructure, maintenance contracts, catering, janitorial services and maintaining on-hand supplies.

Facility support involves more than logistical support. It also involves gaining financial support for the EOC. In tough economic times, emergency managers and practitioners may find it hard to gain funding to develop or improve an EOC. Funding plays a critical role in planning to build or expand an EOC. Gaining support from officials is the main way to secure funding. Additionally, federal funding may be available for EOC planning.

With hybrid or virtual models, facility support becomes more complex. If staff are working from home, there is not an expectation of janitorial or catering services, and other responsibilities such as having personal protective equipment (PPE), backup power or high-speed internet become the responsibility of individual staff members. A necessary consideration for agency leadership is the provision of necessary equipment and supplies (such as docking stations, multiple monitor setups and other peripherals) or financial stipends to limit the burden of the virtualization shift on staff members. IT support becomes critical for both hardware and software. Virtual or hybrid models may also provide greater flexibility in terms of financial support—software as a service (SaaS) may allow for rapidly expanding or contracting licenses.

2.6. Plans and Procedures

The capability assessment should address whether an EOC's plans and procedures—whether the EOC is in development or in place—adequately address the risks and hazards identified in the hazard and vulnerability assessment. These plans and procedures should cover activating the EOC, notifying key personnel to report, staffing the EOC around the clock, providing for Continuity of Operations (COOP) and deactivating the EOC, including producing after-action reports. For more information, visit https://www.fema.gov/continuity-resource-toolkit. These plans and procedures should consider physical, hybrid and virtual EOC environments.

2.7. Communications

EOC leaders should assess the EOC's ability to communicate with the whole community.[4] This assessment should include jurisdictional departments, agencies, organizations and partners, including first responders, first receivers, public health personnel, transportation, public works assets and the general public. EOCs should also consider their capacity to communicate with other levels of government, neighboring jurisdictions, regional partners, private industry and other response and recovery partners. The capability assessment should include items such as alert and notification equipment, warning systems, communications systems, hazard analysis and monitoring, action tracking and resources management.

[4] For details, visit https://www.fema.gov/whole-community.

2.8. Lifelines

EOCs should assess their ability to monitor and support community lifelines, which focus on critical survivor-centric needs. FEMA developed the community lifelines concept in coordination with whole community representatives to increase effectiveness in disaster operations and better position the agency to respond to catastrophic incidents using plain language information-sharing and reporting. EOCs monitor and support community lifelines by creating stabilization targets. More information can be found in the Lifelines Community Toolkit.

The community lifelines concept allows emergency managers and EOCs to:

- Characterize an incident and identify the root causes of priority issues;
- Clearly communicate issues with partners and stakeholders;
- Distinguish the highest priorities and most complex issues; and
- Promote data-driven decision-making.

The lifelines focus on the following areas: Safety and Security; Food, Water, Shelter; Health and Medical; Energy; Communications; Transportation; and Hazardous Materials. For more information, visit https://www.fema.gov/emergency-managers/practitioners/lifelines.

Figure 3. Icons for FEMA's Community Lifelines

Site Selection

This section focuses on criteria for selecting an appropriate physical EOC location. Site selection and EOC construction should abide by state and local building codes, Americans with Disabilities Act (ADA) standards, Environmental Protection Agency (EPA) guidelines and any applicable grant requirements.[5] This guide outlines several elements and attributes leaders should consider when assessing a site's fitness and suitability to serve as an EOC. To save time and money, jurisdictions may identify existing structures that could serve as EOCs before considering new construction.

Consider either converting a vacant structure into an EOC or improving/expanding an existing EOC.

1. General Considerations

1.1. Vulnerability

The biggest consideration in EOC site selection is avoiding potential hazards. For example, it would be counterproductive to locate EOCs in flood plains, on seismic hazards such as faults and liquefaction zones, in potential tsunami and storm-surge inundation zones or in high-risk structures, where they may sustain damage during the very incidents they need to respond to. Of course, no location is risk-free, and jurisdictions may find that each potential site has its own risks.

Jurisdictions should use the results of their hazard and vulnerability assessments to determine which hazards pose the greatest risk. They can then select a site based on its probable resilience to those risks, along with any financial and logistical constraints. For example, EOCs in earthquake zones must be capable of withstanding a major earthquake. EOCs in hurricane-prone areas must consider storm surge and wind speeds.

Consider smaller, more localized hazards in addition to larger risks facing the jurisdiction. For example, look for sites that will see minimal debris from collapsing buildings or failing structures. This is important for urban EOCs, which may be in a courthouse basement or near a high-rise. Do not locate EOCs near high-risk locations, structures or infrastructure elements, including airfields, airports, railroads, high-voltage power lines and pipelines.

Avoiding hazards may be challenging when using the hybrid or virtual models. Because locations such as individual stakeholders' primary and secondary homes and offices may become operating locations, considerations should be made on most likely hazards for each. Efforts should be made to avoid operating in locations with significant risk, and criteria may be established by leadership on stakeholders authorized to operate virtually based on vulnerability. Stakeholders should develop

[5] For information about ADA standards, visit http://www.ada.gov; for EPA guidelines, visit http://www.epa.gov/lawsregs.

contingencies for locations which are extremely vulnerable. One contingency may be to relocate from a home or office to a physical emergency operations center.

1.1.1. CONGRESS PASSED THE DISASTER RECOVERY REFORM ACT (DRRA) OF 2018 TO REDUCE FEMA'S COMPLEXITY AND ENHANCE THE NATION'S CAPACITY TO RESPOND TO FUTURE CATASTROPHIC EVENTS.[6] DRRA SECTION 1206 AMENDED SECTIONS 402 AND 406 OF THE ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT. THE AMENDMENT AUTHORIZED FEMA TO ASSIST SLTT GOVERNMENTS TO HELP ADMINISTER AND ENFORCE BUILDING CODE AND FLOODPLAIN MANAGEMENT ORDINANCES, INCLUDING ASSESSMENTS FOR SUBSTANTIAL DAMAGE COMPLIANCE.CENTRAL LOCATION AND PROXIMITY TO KEY PERSONNEL

To enable a fast response to all parts of the jurisdiction, leaders should locate the EOC centrally and ensure close coordination with the Joint Information Center (JIC). The location of both the EOC and the JIC should enable emergency management officials and response personnel to respond quickly to:

- The EOC itself (when in a physical location);
- The operational needs of the EOC (whether in a physical or virtual location); and
- Affected areas.

Hybrid or virtual environments warrant additional planning measures when looking at location and proximity to key personnel. Virtual environments allow for the inclusion of staff outside of an impacted area, in different time zones, or even in different countries. Personnel outside of the impacted area may have more reliable access to communications and may not be personally impacted by the incident. The ability and availability of key personnel to work in a hybrid environment differs by position; logistics staff may need to physically issue PPE, whereas planning staff may be able to conduct planning meetings virtually. Jurisdictions and organizations with limited staff may be limited by a hybrid or virtual environment as they may be required to fill multiple off-site support and on-site operations roles simultaneously.

Hybrid or virtual environments may provide additional opportunities to assist agencies in their efforts to recruit and retain qualified and diverse staff for emergency operations.

1.2. Traffic Flow and Congestion

Ideally, the EOC will be located in an area with limited traffic, so that routine congestion cannot affect EOC operations. While this is not always possible because of high population density or the EOC's

[6] For more information, visit https://www.fema.gov/disaster-recovery-reform-act-2018.

central location, traffic studies or traffic limitation methods (such as modified traffic-light patterns or expansion of existing roads and infrastructure) can reduce traffic problems during incidents.

Select a site with minimal traffic congestion and chokepoints (for example, avoid inadequate thoroughfares and bridges). Additionally, ensure that the EOC will be accessible even following catastrophic incidents. For example, in an earthquake zone, locating the EOC near a bridge or overpass may cut off access to the EOC after an incident, hindering activation and staffing.

1.3. Accessibility

For ease of access during an incident, locate the EOC near an adequate road network. Consider any hazardous commodities to be transported on main roads or interstate highways, ensuring that a HAZMAT incident will not impede emergency operations. In addition, ensure multi-road access to the EOC, allowing emergency personnel to enter and exit the area freely in the event of road blockage or incident-related traffic or debris.

Accessibility to a hybrid or virtual EOC may be thought of in terms of internet accessibility or access to critical applications (sometimes with the use of virtual private networks). Internet availability and accessibility is typically diminished during all hazards. A benefit of a virtual EOC is the ability to remain connected from disparate locations despite hazard impact areas.

Hybrid and virtual models add numerous other accessibility considerations. With many additional locations where stakeholders may be remotely operating, planning on primary and alternate routes to and from a physical EOC and/or other critical locations should be conducted. Stakeholders with vulnerable operating locations should refrain from using those locations during higher risk timeframes to reduce the possibility of a loss of accessibility (e.g., coastal vacation home during hurricane season).

1.4. Parking

The EOC should provide adequate and secure parking. Planners should ensure that the site can accommodate more than the number of vehicles anticipated during full activation. In multi-jurisdictional incidents, ensure parking for federal and state liaisons. Additionally, provide parking for guests such as the media on EOC and JIC premises.

1.5. Communications

The EOC location should provide strong radio transmission and reception. This is particularly important in rural areas with significant relief in the landscape. The locations of cell and radio towers, both in relation to the EOC and in relation to each other, play a large role in ensuring continuous communications. Planners should conduct a communications study before site selection to ensure acceptable communications capability.

In addition, web-based, interoperable, scalable, flexible and emergency management software tools (e.g., WebEOC) are also critical, as are geospatial and visualization tools (e.g., ArcGIS Online) and

web-publishing tools for public facing communications. Platforms like these support multimodal communications, incident management and collaboration across partner departments, agencies and organizations. Look for more IT requirements below, in the sections titled EOC Capabilities and Requirements, Room Design Features and Information Management Systems.

Hybrid and virtual models should consider fixed broadband internet access and bandwidth to all stakeholder operating locations. Because modern virtual incident management systems can be accessed on most mobile devices, cellular broadband coverage and bandwidth should be considered by users looking to operate remotely.

1.6. Security

Locate the EOC in an area that is easy to secure. Keeping EOC staff safe and protecting communications and support systems are particularly critical. Carefully plan security solutions to maintain the aesthetic quality of the EOC's surroundings so that residents and visitors feel welcome, comfortable and safe. Keep security design in tune with the community context and objectives, rather than focusing solely on individual project objectives. Community-based solutions that encourage community participation in the project design can ensure that the EOC respects and perhaps even enhances its neighborhood. Note, however, that not all elements of the security plan can be shared with the public. Use discretion in dispensing security information.[7]

In a hybrid or virtual EOC, individual staff members may be responsible for security measures. This may include securing sensitive paperwork at home, multi-factor authentication on devices, and identifying secure spaces to conduct meetings when privileged or sensitive information is discussed. The cybersecurity of devices is also a concern; a plan should be in place to ensure critical updates to devices when outside of trusted networks.

Beyond the physical security of hybrid or virtual EOCs, stakeholders must be vigilant in their use of collaboration software. Ensuring videoconferencing applications are password protected, guest access is restricted, and staff are experienced in moderating meetings becomes critical.

1.7. Scalability

Leaders should select the EOC site with long-term growth in mind, particularly in smaller towns and rural areas. EOC space needs will vary based on the type of emergency or the stage of response. As a result, EOC sites should be expandable to meet different contingencies.

EOC sites that serve as training facilities or that house fire service vehicles or law enforcement facilities should accommodate growth plans for all site occupants. This may call for a design that accommodates building expansion, warehouse growth, additional parking, etc. In situations where

[7] For more information, see FEMA 430: Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks, 2007.

EOC construction funds are limited, designing for growth allows for future expansion of a facility once funds become available.

In a hybrid or virtual EOC, scalability may require additional pieces of hardware and increased software licenses both internally with staff and externally with other key stakeholders. License expansion may be used outside of the EOC such as in virtual joint information centers and department operation centers. Considerations about demobilization and contracting license requirements should also be part of the planning process.

The hybrid and virtual models enable physical EOCs to expand with additional staff without the need for additional workstation space. Jurisdictions and organizations should consider these models to enhance their scalability of primary physical sites.

1.8. Community-Based Design

In constructing an EOC facility, jurisdictions should not alter listed or nationally designated historic sites or structures. Planners should consider the proximity of protected historical sites or structures to a proposed EOC location during the site selection process. This sensitivity also applies to building design. As EOCs are functional buildings that will be in place for a long time, the design of the facility should reflect the community's architectural values. Design and landscaping should blend with the local community rather than stand out from it.

1.9. Alternate Sites

If an EOC proves unable to support an emergency response effort, the jurisdiction should identify an alternate EOC with capabilities equal or greater than the primary EOC. Having a preselected and prepared secondary site, together with relocation plans, will enable an EOC to relocate quickly and seamlessly. A mobile unit equipped with communications capabilities greatly enhances an EOC's ability to relocate without seriously degrading its coordination and control functions. Leaders should consider planning for an alternate facility while developing the primary EOC. In addition, by planning for an alternate site, planners may identify opportunities for minor design changes that would ease migration to an alternate site. For example, the planner could consider using mirrored servers or telephone switchovers.

COOP plans should specify who can activate alternate sites, why and how they should activate them and how the jurisdiction will notify people about the activation. Each of these components should become part of routine training and exercising of alternate EOC sites. This preparation will assist in the efficient transition to an alternate site in an emergency.

Virtualization of emergency operations centers enables many additional opportunities for alternate platforms to manage incidents. Where historically an alternate EOC may have been another physical site, it may be determined by the agency that a virtual EOC may be an effective alternate solution instead. Virtual EOC systems may be an effective temporary solution while the alternate physical site is being activated. The more familiar staff and stakeholders are with the tools and systems used in a

virtual EOC, the more effective they will be using them in continuity of operations incidents. Even during the activation of a physical alternate EOC, there may be a need to access virtual EOC services. Plans should consider access to these systems for all alternate EOC locations.

1.10. Existing EOC Sites

The most important thing to consider when enhancing or updating an existing EOC is how to optimize the space and technology available. The EOC Capabilities and Requirements section of this guide, below, discusses planning an EOC update.

2. Mitigation Considerations

2.1. Natural Hazards

Most potential EOC sites have one or more potential natural hazards. Jurisdictions should consider natural hazards and select a location that minimizes their potential impact and improves operational resilience. These hazards include earthquakes, flooding, wind, wildfire, mudslides, disease outbreak and sinkholes.

2.2. Technological and Human-Caused Hazards

Leaders should also consider technological and human-caused hazards when selecting a site. The site should minimize the potential impact of hazards such as chemicals, nuclear power plants and terrorism.

2.3. Virtual and Hybrid Operations

If an EOC is in an area susceptible to natural, technological, or human-caused hazards, a consideration for hybrid or virtual EOCs may be to identify staff in geographically separated areas where virtual operations can be continued. This philosophy is like how large organizations manage data center and cloud provider redundancy. National and international organizations may have other office sites outside of areas at risk of certain types of hazards where staff are located that could support operations. Local, state and regional organizations may establish mutual aid agreements with organizations in areas that may not encounter similar hazards in order to utilize staff for functions that can be done remotely.

EOC Capabilities and Requirements

This section discusses how jurisdictions use preliminary assessments (especially capabilities and needs assessments) to identify design requirements for the EOC. It also discusses the need to compare the capabilities and requirements with the jurisdiction's Emergency Operations Plan (EOP) to ensure that the EOC will meet the jurisdiction's needs.

1. Determining Personnel Space Requirements

1.1. EOC Functions

EOC functions and activities drive design and layout considerations. An EOC's key activities include the following:

- Authorizing EOC activation;
- Directing EOC operations;
- Gathering and providing information;
- Identifying and addressing issues;
- Providing internet connectivity and ensuring interoperable communications capabilities among all partner agencies and organizations;
- Response planning and future planning; and
- Demobilizing EOC management.

Each key activity comprises critical tasks. In turn, each critical task has resource requirements (personnel, equipment and supplies). These resource requirements drive EOC design. A crucial step in designing an EOC is to determine which capabilities are necessary for the EOC and to use this information to establish design criteria.

Some EOC functions may happen offsite. For example, the JIC may or may not be co-located with the EOC. The site plan must therefore support operations at the EOC while also considering the need for connectivity to remote locations.

1.2. Space Requirements

Planners should consider both minimum and maximum staffing levels, including staff necessary to sustain 24-hour operations. Staffing numbers should include any liaisons from other agencies or levels of government who may arrive in response to an incident.

1.3. Additional Personnel Space Requirements

Planners should consider the need for support services, restroom space, meeting space and a "quiet room" for stress counseling. Ideally, personnel will also have designated areas for meals, rather than having to eat in their workspace, as well as a space set aside for breaks and relaxation, where feasible. Storage for emergency food and water supplies is also necessary. Finally, planners should consider the need for executive office space.

1.4. Sustained Operations

Another consideration is the length of time that the EOC may have to self-sustain. For example, under many circumstances, EOC staff can use an outside catering service. However, if the hazard and vulnerability analyses suggest that there may be periods of isolation, the EOC must have enough food and water on hand to sustain the staff. Where feasible, planners should consider the need for well-functioning on-site shower facilities (fixed or temporary).

In addition to food, water and hygiene, planners must consider the need for sanitary supplies and office products during a period of self-contained operation. Sanitary supplies can be bulky and take considerable space. These supplies are even more important during a pandemic.

In a hybrid or virtual environment, it should be clearly communicated what the expectation is of virtual staff at locations outside of a physical EOC. Determining if supply kits/stay kits are required, how long staff can sustain operations virtually, when remote stakeholders would be required to relocate to the physical EOC, or if the EOC is required to resupply staff members are all considerations.

2. Communications Requirements

The EOC's ability to function depends on its ability to communicate. Planners must therefore consider several challenges involved in maintaining a functional communications system. Voice and data communications in and out of the EOC must be reliable to ensure that information and critical decisions can transfer quickly to the correct personnel. The EOC design must also facilitate face-to-face communication to optimize EOC efforts.

Not all EOCs have the same communications requirements. Planners should tailor the communications infrastructure to support both internal and external functional needs, integrated with other emergency management elements. Some areas have opted to use amateur radios.

The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen and enhance emergency communications capabilities. The NECP provides guidance to those that plan for, coordinate, maintain, invest in, and use communications to support public safety operations. For more information on the NECP that may support planning for communications requirements, visit: https://www.cisa.gov/necp.

2.1. Interoperability

A jurisdiction's primary response communications systems typically include police, fire and medical services radio systems. These first responders are accustomed to communicating with each other and with 911 dispatchers, whether or not the 911 center is co-located with the EOC.

A more pressing concern is integrating expanded emergency operations to include agencies that respond alongside first responders. These include first receivers at hospitals, triage centers, mass care shelters, special needs shelters, educational facilities and the specialized operations centers that coordinate operations centers for various state, county and municipal agencies. Among these agencies are traffic control centers, public health operations centers, transportation dispatchers, transit agency operations centers, fusion centers, JICs, etc.

In a hybrid or virtual environment, interoperability will also include system interoperability for virtual collaboration or operations software (e.g., Microsoft Teams, Google Workspace, Slack, Zoom, Cisco WebEx Meetings etc.). Interoperability may also include data interoperability when sharing files or geospatial resources. Finally, hybrid or virtual environments have the aggravating factor of agency firewalls, incompatible software and hardware, and general IT policy limitations.

2.2. Telecommunications (Including Teleconferencing, Videoconferencing, Text Messaging and Fax)

The EOC should have adequate telephone extensions and fax capabilities for full operations. Planners should consider landline capabilities, Voice over Internet Protocol (VoIP), video relay systems, digital systems and other reliable voice and data communications options as a primary system. Text messaging can assist with communications, as it provides an immediate avenue for written communication. SMS (short message service) is a text messaging service component of most telephone, internet and mobile device systems. In some events, text and SMS may have a higher reliability and transmit quicker than voice.

Cellular and pager service is important, when available, not only for activation and on-call personnel, but also for personnel who are working remotely or traveling among neighboring EOCs, joint field offices (JFOs) and incident scenes. Consider cell phones with two-way radio capability, as well as technology such as cell phone signal boosters/repeaters. Remember that cellular and pager service depends on both power and intact cellular towers. Additionally, the load on the network plays a significant role in subscribers' ability to communicate. During some incidents, cellular and pager service will not be available. As necessary. the EOC should stock satellite mobile phones if in a remote area, where there are no landline or cellular telephone networks or in an area where existing networks are damaged or overloaded.

Telecommunications becomes even more important in a hybrid or virtual environment where face-to-face communication is limited. Ensuring staff still have cellular and pager service at their home or alternate location, as well as satisfactory bandwidth to participate in or facilitate teleconferencing or videoconferencing systems is critical.

2.3. Public Safety Radio

EOC planners should consider several factors related to public safety radio. For example:

- Will agencies provide their own radios, or will this equipment be part of the EOC project?
- Will the installation be temporary (requiring handheld radios) or permanent (requiring a radio base station)?
- If agencies provide the radios, will they require power and antenna hookups for extended operations?
- Will radios be available in the Operations Room (Ops Room) or monitored in a separate communications room?
- Will different radio systems create interference with each other?
- Does the EOC have enough electrical outlets for all the expected equipment?
- Will a radio repeater be necessary to retransmit and extend radio frequencies?
- Are chargers necessary for radios, cell phones, pagers, etc.?

In hybrid and virtual models, access to public safety radios may be limited. Organizations should consider availability of portable radios, chargers and accessories for all who need land mobile radio access, if their remote operating locations provide necessary radio coverage, distribution and accountability of radios. Alternate and more inexpensive solutions to access radio networks should be considered including Radio over Internet Protocol (RoIP), mobile and web applications.

3. IT Requirements

Understanding the EOC functions allows the planner to determine the technology required to perform those functions. In addition to communications requirements, successful EOC activity relies heavily on modern digital technology.

3.1. Internet Connectivity

The internet offers several essential capabilities often overlooked in EOC planning. EOC public information and media staff need the ability to access and update websites, publish blog posts and provide releases via streaming video and audio. EOC planning should include space and system requirements to enable these capabilities.

As mentioned in the Telecommunications (Including Teleconferencing, Videoconferencing, Text Messaging and Fax) section above, functioning internet capability usually requires power (electricity) and an internet service provider (ISP). IT redundancy considerations are an important part of planning and preparedness. Planners should therefore identify several options and evaluate the

specifications, requirements, capabilities, reliability and cost of each before placing an order. Upon acquiring technology, planners should test it to ensure it is ready for real-world activation. If operating in a hybrid or virtual environment, internet connectivity becomes a single point of failure. Testing mobile wi-fi hotspots, portable routers and boosters, or mobile broadband sticks at alternate sites, as well as identifying backup ISPs or alternate technology such as satellite internet should be considered. Connectivity options include the following:

- Mobile Wi-Fi hotspot: This portable device allows users to set up an internet connection almost anywhere. It works by taking a long-term evolution (LTE) wireless broadband signal from a cellular network provider and converting it to a Wi-Fi signal that a laptop computer or smartphone can use;

- Portable routers and boosters: Portable routers transfer data, via internet protocol (IP) packages from a given source, to create an internet hotspot. Wi-Fi boosters extend the range of the existing Wi-Fi in a location by receiving the wireless signals from the router and repeating them with powerful amplifiers and antennas;

- Mobile broadband USB stick: This compact device connects a computer to a cellular data network, providing internet access in the same way that a smartphone does. The device plugs into a computer's USB port and looks like a memory stick or flash drive;

- Internet by satellite: Orbiting satellites provide an alternate way to access all-location internet and phone communication networks. Because the service does not rely on land-based internet infrastructure, it is less vulnerable to outages caused by cellular dead zones and incidents such as fires and hurricanes; and

- Relocation: Relocating to a designated secondary or alternate EOC location is another way to restore connectivity.

Considerations should be made for systems and software that provide some functionality without internet connectivity. During a disaster, internet connectivity may be intermittent or non-existent. Systems should be able to store data locally with the ability to sync when connectivity is restored.

3.2. Computer Systems

In developing EOC computer systems, the planner starts by considering the functions users will perform. This information provides insight into the number of computers necessary and the potential processing load on the system. It also informs decisions related to connectivity, such as the use of wireless versus wired systems, and processing, such as the use of server-resident versus standalone software.

Another important consideration is whether to temporarily remove firewalls and internet blocks during an emergency. Some organizations block access to certain websites (such as social media sites) during normal operations, but allow access to them in an EOC, knowing they may be useful. If

the organization permits and authorizes, approved EOC personnel may arrange to have such restrictions removed from computers located in or activated during EOC operations.

In hybrid or virtual environments, the expected length of activation may help determine the need to transition to laptops or to relocate fixed systems to alternate sites. Coordination with IT will help inform the EOC on security concerns, updates and patches, and access to critical applications.

Also consider virtual machine and cloud-based computer technologies. These allow staff to access their desktop environment from any device (mobile, other operating systems, TVs, etc.) and any location while gaining immediate access to their applications and documents.

3.3. Audiovisual Support

Display capacity is an important part of a modern EOC. Audiovisual display options range from simple projectors to elaborate closed-circuit television systems. Many incident management programs now make status information (including television and radio broadcasts) available to individual users, which potentially reduces the need for elaborate display systems. Managers should consider the use of closed-captioning or visible sign language interpreters, as necessary. Audiovisual systems should be able to accommodate hybrid and virtual models where staff may simultaneously be in the EOC and at alternate sites.

4. Supplies and Equipment Requirements

After leaders have determined the layout of the EOC, they define the requirements for non-fixed equipment, supplies and rations, as described below.

4.1. Furniture and Office Equipment

EOCs provide all necessary furniture and office equipment. When possible, planners should procure folding or collapsible items to reduce necessary storage space and consider furniture that is easy to transport and move. Planners should also obtain furniture and equipment for staff that requested reasonable accommodations. Staff members operating in a hybrid or virtual environment may not have appropriate office furniture to operate for extended periods including desks and chairs.

4.2. Food Supply

EOCs may feed their personnel in a number of ways, such as through outside caterers, standby contracts with local NGOs that maintain kitchens, donations from restaurants or stored foods—including prepackaged emergency food supplies such as meals ready to eat (MRE) or commercial foods with a relatively long shelf life. Supplied food should meet the dietary requirements of the staff. Staff should ensure that stored food products meet certain storage requirements and should rotate them based on expiration dates. Users operating in a hybrid or virtual environment should consider access and availability of food during extended operations and a need to store meals on site. While

catering is outside the scope of most working remotely, meal delivery services may be a viable solution depending on the incident.

4.3. Medical and Sanitary Supplies

Medical supplies are generally limited. On-hand sanitary supplies should meet the needs of assigned EOC staff for an extended period. Proper, adequate PPE should also be available, along with training or instructions on storage, handling, use, application and disposal. Users operating in a hybrid or virtual environment should consider access and availability of medical and sanitary supplies during extended operations and a need to store supplies on site.

4.4. Status and Situation Boards

Visual displays are important because they provide staff members with immediate access to information without verbal interruptions. Hybrid and virtual environments present numerous opportunities to leverage collaborative services to display situation information. This may include interactive dashboards, maps, Kanban-style card systems, and other virtual whiteboards.

4.5. Administrative Supplies

EOCs should keep enough supplies on hand to conduct efficient emergency operations and support janitorial services for an extended period. Administrators should also keep a hard copy of relevant forms, documents, checklists, etc., in addition to the copies that the responsible parties maintain. While hybrid or virtual environments may reduce the need for paper-based processes, users should consider access and availability of administrative supplies during extended operations and a need to store supplies on site. This may be particularly important in long-term power outages or situations where computer systems are inoperable or temporarily out of service.

4.6. Support Services

Like any other office facility, an EOC requires support services, and the demand for these services may increase during activation. For example, janitorial services usually occur once a day, at night. However, a facility operating 24 hours a day will need more frequent trash pickup and restroom maintenance.

The EOC may also need other support services, such as catering or stress management counseling. The EOC usually orders these services only as necessary, but an on-call arrangement poses a number of potential problems. For example, vendors may not have the capacity to provide services in an emergency, there may be security and confidentiality concerns, and the EOC may become too congested, as too many people try to work in a small space at the same time.

Consequently, EOC managers must decide what services are necessary routinely and what services should increase during activation. Managers should consider adding emergency clauses to existing service contracts and developing standby contracts. Finally, they should identify multiple vendors for critical services.

Users operating in a hybrid or virtual environment should consider the viability of community lifelines to the locations they will be operating from. An extended loss of electricity, potable water, wastewater or trash services at their home or office may require users to relocate to a physical EOC space.

Room Design Features

This section addresses how leaders can place equipment, capabilities and personnel to maximize operational efficiency and effectiveness, facilitate NIMS-compliant operations and support expandable operations. It also addresses multiuse considerations, expandability and continuous operations.

1. Design Considerations

1.1. Basic Room Designs

There are five basic EOC designs: the boardroom, mission control, marketplace, bull's-eye, and virtual EOC.[8] Regardless of the chosen room design, sightlines should be taken into consideration to ensure staff are able to see necessary visuals.

- Boardroom: This is the classic EOC layout in which agency representatives work around a U-shaped table, with the main visual display in the front of the room. Support staff sit behind the main participants, and additional visual displays line the walls behind them. This layout emphasizes collaboration and coordination.

- Mission control: This layout approximates a lecture hall, with staff seated in rows or semicircles facing large visual displays. This layout is heavily dependent on technology, and staff members communicate primarily through incident management software. This layout works well for technical tasks but may limit collaboration and interaction among staff.

- Marketplace: This is another classic EOC design. Staff members sit in separate, function-specific groups (for example, ESFs or ICS units) that emphasize collaboration among specialists. Staff members then need to coordinate across groups.

- Bull's-eye: In this layout, key leaders sit at a main table, with additional staff seated at tables behind them in concentric circles. This arrangement emphasizes the standing of the key players but can limit collaboration. For this reason, and because it is also space intensive, it is not an ideal EOC layout.

- Virtual EOC: This is not technically a layout but rather a means of augmenting the physical layout of an EOC. By creating a virtual EOC through web-based technology, EOC staff can collaborate with other groups and agencies without having their representatives physically located in the

[8] Botterell, Art. A Design Language for EOC Facilities, 2002.

EOC. A virtual EOC can serve as an adjunct to any physical layout. See the example in the box below.

Virtual EOC Example:

National Business Emergency Operations Center

The National Business Emergency Operations Center (NBEOC) is FEMA's virtual clearinghouse for two-way information sharing between public and private sector stakeholders before, during and after disasters.

The NBEOC uses web-based platforms, dashboards and other virtual tools to communicate and coordinate with its members. During emergency operations, the NBEOC provides real-time situational awareness about the incident and the needs of affected people and communities.

FEMA's Office of Response and Recovery, Private Sector Division, operates the NBEOC under ESF #14: Cross-Sector Business and Infrastructure. The NEBOC operates within FEMA's National Response Coordination Center (NRCC).

For more information, visit https://www.fema.gov/business-industry/national-business-emergency-operations-center.

In designing a virtual EOC for successful implementation, operation and continuous improvement, leaders discuss many of the same capabilities and considerations as they do for physical EOCs.

Essential elements include the following:

- Establishing activation, operation and deactivation criteria, processes and procedures with all virtual EOC partners and participants;
- Defining clear roles and responsibilities involved in an activated virtual EOC;
- Conducting partner training and exercises in all relevant virtual EOC operations;
- Ensuring that the technology to support internet connectivity, teleconferencing, videoconferencing, real-time status monitoring, alerts/notifications, telecommunications and mobile/radio communications is available and operational 24/7;
- Monitoring, tracking, reporting and maintaining documentation on event status, personnel and other resources;
- Creating an effective user interface and user experience; and
- Incorporating lessons learned in ongoing, comprehensive virtual EOC planning and coordination.

A number of other design considerations also contribute to an effective EOC. EOC must maintain a COOP to ensure the EOC remains operable. Consider carefully augmenting physical EOCs with virtual components to prevent the creation of "silos" and disconnect between stakeholders working in

person versus those working remotely. When possible, mirror some physical EOC components in the virtual environment such as providing individual/breakout teams and channels, creating “always open/always on” channels for collaboration, or even including emerging technologies such as augmented or virtual reality systems. Contingencies to virtual EOC operations should always be considered, particularly related to power outages, communications failures, technology failures, and intentional cyber attacks.

1.2. Emergency Power

During a disaster, the EOC may experience extensive power outages. Thus, the EOC needs enough emergency auxiliary power (usually in the form of backup generators) to support the EOC’s operations 24 hours a day for an extended period. Leaders should schedule regular backup and maintenance of this system to ensure its functionality under full workload conditions for a full operational period. If staff members are unable to complete this maintenance task, consider contracting with a local vendor.

Testing and training in the use of the backup generators (where applicable) are essential parts of a comprehensive preparedness plan. It is important to know what will and won’t be powered by backup power, such as certain outlets, electronic gates or doors, elevators and HVAC. In addition to training EOC personnel in the use, operation and maintenance of the backup generators, leaders should post the generator operation instructions in a conspicuous location, accessible and known to those trained to operate and monitor the equipment.

Locations used for hybrid and virtual emergency operations should also consider emergency power requirements. Locations should consider the installation of fixed generators, the safe use of portable generators, solar plus battery storage, and other resilient energy systems.

1.3. Uninterruptible Power Supply

An uninterruptible power supply (UPS) is a type of device that powers equipment, nearly instantaneously, in the event of grid power failure, protecting the equipment from damage. UPS systems vary significantly in their design and functionality, and these differences affect their capabilities and cost.

All UPS systems serve two main purposes: They provide backup power as quickly as possible in the event of power loss, and they offer some degree of protection from power quality issues that may damage equipment. UPS systems fulfill these goals to varying degrees depending on their design and features.

Small UPS units typically use batteries to provide power to two to four pieces of equipment for a limited duration (10 to 20 minutes, depending on the load). Planners should ensure that these UPS units can provide backup power for the time necessary to support their assigned equipment until emergency power comes online.

Data servers, computer systems, industrial settings and laboratories all commonly use UPS systems. Because a UPS protects equipment, it is appropriate for any situation where electrical loads may be sensitive to power loss or other power quality issues. For example, UPS systems are commonly used for computers and servers because power loss to these loads may result in data loss or component damage.

While UPS systems and portable batteries may provide power for short-term outages, they likely will not effectively bridge the gap for extended power outages; this will impact virtual or hybrid staff disproportionately. Options such as solar panels coupled with storage packs, home generators, and alternate energy sources may be necessary for virtual operations.

Many telephone systems are now computerized and need a UPS to ensure reliability during power fluctuations. UPS units can also support a phone system either until emergency power comes online or long enough to facilitate an orderly shutdown.

1.4. Physical Access

If the EOC shares access with another organization or other government services, leaders should implement processes to restrict access to operational areas when appropriate. This could include controlling entry to the EOC using a card access system that provides 24-hour access to the facility. Ensure that none of the access control systems (card access, elevators, lock-out stairwells) could prevent access to or egress from the facility if they become nonoperational (for example, if primary and auxiliary power systems fail or network/server outages occur). Planners should also consider security measures for parking areas.

2. Considerations for Multiuse Facilities

Having a dedicated EOC, while highly desirable, is not always feasible, for financial or political reasons. Consequently, some EOCs operate as multiuse facilities. Designing a multiuse facility requires careful thought, as multiuse designs involve a compromise between often opposing interests. For example, office users may demand individual offices, while the EOC favors an open plan layout. The answer to such a conflict lies in defining the primary use.

If the government EOC is co-located or if the facility housing the EOC is multiuse, users from different organizations can share many areas of the building, provided appropriate access control precautions exist for operational areas. A summary of shared and exclusive spaces and rooms follows.

2.1. Ancillary Space and Storage Areas

The EOC can share ancillary and storage areas with other government functions during periods of inactivation, but EOC personnel must have easy and rapid access during times of activation. These spaces can include supply closets, janitorial closets, hallways, conference rooms, etc. In some cases, climate-controlled storage may be needed for electronics and network elements. Policies on shared areas should state that during periods of activation at a certain level, EOC needs take priority. If this

is not possible because of activities within the shared building, the jurisdiction should consider alternate plans.

2.2. Operations Room

The EOC should reserve its Ops Room—home to its displays, equipment and emergency functions—for activations and other scheduled activities, such as authorized classroom training. The Ops Room should not become an informal workspace or overflow office space.

2.3. Classroom and Training Areas

Classrooms and training areas independent of the Ops Room can serve as operational sleeping or feeding areas during emergency activations. If this is the intent, the design should reflect a number of considerations, including proximity of restrooms; access to lockers for personal belongings; storage for cots, folding tables and other furniture; and overhead lighting designed to accommodate sleep and quiet activity in different areas of the room. An architect can advise planners on additional requirements, including design and fire code requirements for sleeping quarters.

2.4. Meeting Rooms

Large EOCs normally need nearby conference facilities where key emergency personnel can discuss priority problems away from the noise and disruption of the Ops and Communication rooms. If these conference areas are shared, they should be marked as intended primarily for the EOC's use (under mutually agreed-upon criteria, terms and conditions). Leaders should establish procedures that give the EOC immediate priority access during emergency operations.

3. Floor Plans

The arrangement of furniture and equipment in an EOC often changes following a call to action. Leaders should post floor plans and train personnel to arrange spaces so that EOC operations can begin as quickly as possible following disasters, incidents and events.

Where possible, planners should keep the floor plan flexible and consider the following:

- Provide at least twice the number of outlets and network drops necessary in a given EOC;
- Indicate the location of ports for internet, telephones, satellite phones and radios. Label on floor plan as well as any physical labeling that can be done. Specify which ports are generic/specific, and which ports are always working or require patching;
- Allow for accessibility for those with disabilities or access and functional needs; and
- Use moveable furniture and hide cabling in a suspended floor or ceiling to protect against trip hazards. (If furniture is not moveable, fixed electrical and communications outlets are fine, and outlets do not have to be visible.)

Information Management Systems

This section discusses the handling and transfer of all information related to an incident, including sensitive information and secure communications.

1.1. Information/Data Management Tools

Effective emergency response involves knowledge of critical information that can help inform an appropriate response. The following tools and capabilities are examples that may be useful during an emergency response:

- Geospatial data and analysis capability: Will the EOC have access to geospatial information for the jurisdiction—maps, imagery or GIS?
- Crowdsourcing in emergency management: Will the EOC have the correct skillset to conduct crowdsourcing? Will the EOC have queries set up in advance of an incident?
- Hazard prediction and monitoring capability: Will the EOC have hazard prediction capabilities (models) that can plot and predict downwind hazards for chemicals or radioactive fallout? Will the EOC have hazard protection capabilities (models) and monitors for natural hazards—for example, flood gauges, tsunami warning systems or seismic monitoring systems?
- Crisis information management system: Will the EOC have a crisis information management system that integrates the necessary information so users can access it quickly and efficiently?
- Personnel qualification and certification system: Will the EOC have a system to track qualified and certified personnel within the jurisdiction?

1.2. Geospatial Data and Analysis Capability

Knowing the precise location of buildings, roads and critical infrastructure is essential to an effective response. The EOC should have the capability to access geographical information quickly and effectively. This information can take the form of specialized databases or incident logs that list critical infrastructure. See the discussion of RAPT in the Preliminary Assessments section above for more information.

This information is important in dispatching first responders, determining evacuation routes and securing areas during events such as civil unrest and bomb threats. When combined with adequate hazard prediction and monitoring capabilities, geospatial information provides a powerful capability to identify at-risk populations during hazards such as flash floods, tornadoes and downwind chemical hazards. Precise information about buildings can also help identify facilities that may require a large-scale evacuation (for example, long-term care facilities, schools, hospitals and prisons).

Access to geospatial data and products may be dependent on your licensing model. On-premise and enterprise solutions typically offer greater control, but cloud-based solutions can scale rapidly for large events. Consider remote user access to on-premise GIS servers if they are not on organizational networks. In addition, some GIS tools and software require significant processing power which may require a higher-end computer for some staff.

1.3. Crowdsourcing in Emergency Management

Crowdsourcing is a method for gathering open-source ideas, content or services produced by many people scattered across the digital world and then curating this data into consumable and informative products. Digital volunteer networks (DVNs), which lead specific crowdsourcing efforts, are the virtual equivalent of field-based voluntary organizations.

These networks perform crowdsourcing by dividing the collection, analysis and visualization of data between trained volunteers who have experience in fields such as mapping, coding, communications and social media. The resulting products provide emergency managers with increased situational awareness and identify resource gaps based on data that would have otherwise been untapped. In many cases, crowdsourced data is more accurate and faster to obtain than traditionally sourced data.

FEMA's NRCC Crowdsourcing Unit acts as a liaison between the emergency management community and DVNs. The NRCC generates requests for crowdsourced products based on critical information gaps that can inform sound decision-making. During disaster activations, the Crowdsourcing Unit maintains digital communication channels and hosts daily coordination calls with DVNs to communicate disaster response priorities, gain situational awareness of DVN crowdsourcing efforts and facilitate critical information sharing.

During the 2017 hurricane season, FEMA used crowdsourcing by coordinating with DVNs and organizing two disaster hackathons. These efforts showed that crowdsourced data, tools and services can enhance situational awareness and decision-making. Crowdsourced data is also critical for improving machine learning and artificial intelligence applications that can enhance emergency response efforts. For more information on FEMA's crowdsourcing efforts and initiatives, visit https://www.nysgis.net/wp-content/uploads/2019/04/FEMA-Crowdsourcing-Unit-One-Pager_508.pdf.

FEMA's NRCC Crowdsourcing Unit

During NRCC activations, FEMA's NRCC Crowdsourcing Unit identifies impacts to critical lifelines through two types of activities:

- Active crowdsourcing—by coordinating with DVNs to develop crowdsourced products specific to the disaster
- Passive crowdsourcing—by using existing crowdsourcing platforms and social media monitoring tools developed by the private sector tech industry

1.4. Hazard Prediction and Monitoring Capability

Hazard prediction encompasses an EOC's ability to predict and monitor impending or existing hazards. This capability may include computer modeling for chemical or radioactive hazards, as well as the ability to monitor streams, severe weather, hurricanes and earthquakes. Weather monitoring capability (temperature, wind speed and rainfall) can help users predict and track natural hazards, such as mudslides, wildfires and flash floods. The jurisdictional hazard and vulnerability assessment identifies hazards that may require prediction and monitoring capability at the EOC. Since EOCs vary in size, scope and capability, EOCs may or may not have staff trained in and familiar with hazard prediction and monitoring capability. FEMA recommends that EOC leaders consider hazard prediction and monitoring training and expertise when recruiting staff and assessing skillsets. When this expertise is not available within the EOC, consider establishing partnerships with this capability in the region.

In a hybrid or virtual environment, ensure access to modeling applications, sensitive plans and procedures (e.g., dam emergency action plans), live feeds from stream gauges and weather stations, and other hazard prediction and monitoring capabilities are still accessible.

1.5. Crisis Information Management System

A crisis information management system may consist of open-source, free, or commercial, off-the-shelf software, often with additional applications for specialized needs. The system should manage key information such as GIS information and hazard prediction models. A crisis information management system should help users manage the incident and track resource deployment, response teams and other response capabilities, according to the jurisdiction's plan. It should also manage diverse data elements such as threat assessments, status reports, incident alerts, contingency plans, response plans, damage assessments, supplies, personnel data (including certifications and phone numbers), recovery plans and incident logs.

While a commercial, off-the-shelf system is not a requirement, each EOC should have a good file management system, with logical, intuitive file locations and naming conventions. Remember that systems can fail, so electronic and hard copy backup methods are important.

Consider utilizing automated processes to track, approve, and archive documents, as well as satisfy records retention policies. Data storage, security, access and interoperability amongst crisis information management systems is also critical. Like many software solutions, crisis information management systems may be hosted on-premise or in the cloud. If using an on-premise solution, considerations must be made for hybrid or virtual users to ensure secure access to the system from their devices. While there are many purpose-built crisis information management systems on the market, organizations should consider other cloud-based collaboration and project management tools with similar functionality for their virtual emergency operations center. In some cases, their organization or jurisdiction may have already invested significant resources to acquire licenses and conduct training for staff members on these commercial off-the-shelf solutions, helping to increase likelihood of adoption by all stakeholders without having to learn a completely new system.

Interoperability between crisis information management systems should be considered, as various jurisdictions and organizations may be utilizing the same brand of system, although there is no ability to share information, resource requests or files between each.

1.6. Personnel Qualification and Certification System

FEMA developed NQS as a supplement to the Resource Management component of NIMS. NQS establishes guidance and tools to assist stakeholders in developing processes for qualifying, certifying and credentialing deployable incident management and support personnel. NQS can help EOCs build or refine qualification, certification and credentialing processes, making them effective and consistent nationwide. NQS establishes standard minimum qualifications for specific incident-related positions to provide consistency across the nation and support nationwide interoperability. Using the NQS approach ensures that personnel deploying through mutual aid agreements and compacts have the capabilities to perform the duties of their assigned roles. For more information on NQS, visit https://www.fema.gov/emergency-managers/nims/components#nqs.

OneResponder, the application supporting NQS, is a web-based master qualification system that provides a common language and approach for qualifying and certifying emergency personnel. OneResponder allows users to customize position qualifications, create resource catalogs, establish and maintain data-sharing networks with other participants and collaborate on master resource catalogs. It is designed to support the development of a national incident workforce. For more information on OneResponder, visit https://preptoolkit.fema.gov/web/national-resource-hub/personnel-qualifications/.

2. Infrastructure for Communications and Data Management

The communications and data management infrastructure represents the backbone of EOC operations. Resilient communications systems, including voice and data circuits, local computer networks and connectivity to the internet are essential to the EOC's coordination and management function. Planning and implementing proper infrastructure will allow EOC operations to function properly.

2.1. Adequate Numbers of Phones, Multifunction Copy/Scan/Print/Fax Devices, Copiers, Computers

EOCs should have enough phones, internal directories, fax machines, photocopiers, computers and plotter printers (when and where feasible) to support regular staff, additional personnel from partner agencies and surge personnel from various agencies who may be present during an emergency. In addition to physical equipment, the EOC should consider the space needs to accommodate additional personnel. As operations expand, personnel often spread into rooms previously used for normal, non-operations activities. Emergency managers should consider the space requirements for emergency operations—and the need for as much flexible operational space as possible. Stringing

extra phone lines together or making use of raised floors can enhance the flexibility of a facility's available space. Useful computer peripherals to maximize computer work performance such as multiple monitors, webcams, or headsets should also be considered in and out of the physical EOC. Organizations should consider how to distribute these peripherals in advance for stakeholders that may not have access on their personal computers at home. Some organizations provide some access to "bring-your-own-device" laptops, although many only authorize devices owned by the organization to be used for work purposes. This should be considered in the event virtual emergency operations must be scaled up quickly to include non-traditional stakeholders without access to organization-furnished devices.

2.2. Secure Communications

Sometimes, especially during emergencies, EOCs need to send and receive highly sensitive information requiring secure communications. Secure data communications capabilities are critical, including secure audio transmission capabilities. Additionally, rooms with secure communications equipment need higher physical security measures to ensure that only authorized personnel have access to the equipment. EOCs that may need to conduct classified business should develop policies for how staff must return to an appropriately outfitted physical EOC or office space when secure communications are needed.

3. Cybersecurity

EOCs should protect their systems against physical and cyber risks (e.g., unauthorized access, denial of service, ransomware). As cyber threats and vulnerabilities grow in complexity and sophistication, incidents become more numerous and severe against EOCs. Therefore, it is critical that EOCs take proactive measures to carefully manage their cybersecurity risks. Establishing cybersecurity risk management can help EOCs identify and prioritize risks, protect resources, detect threats, and enable coordinated, effective response and recovery. Despite every effort, cyber incidents will occur. EOCs should be prepared to execute response processes and procedures, prevent expansion of the event and mitigate its effects. Incident response plans, recovery or resiliency plans, and continuity of operations plans are useful in a cybersecurity incident response. Recovery planning processes and strategies are improved by incorporating lessons learned into future activities. Response personnel should be trained on the latest security, resiliency, continuity, and operational practices and maintain in-service training as new technology and methods are made available.

The Cybersecurity and Infrastructure Security Agency (CISA) works closely with public, private sector and international partners, offering technical assistance, information security and education to protect our nation's critical infrastructure from a broad range of current cyber, communication and physical threats. For personalized support, visit CISA Central at https://www.cisa.gov/central. For detailed cybersecurity guidance and best practices, visit the Publications Library at https://www.cisa.gov/publications-library and subscribe to National Cyber Awareness System products at https://www.cisa.gov/uscert/ncas.

To improve EOC communications and cyber resiliency, visit:

- Public Safety Communications and Cyber Resiliency Toolkit: Assists public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency and developing plans for mitigating the effects of potential resiliency threats. Within the Toolkit, the Cyber Resiliency Resources for Public Safety Fact Sheet highlights resources provided by the federal government, industry and trade associations. The factsheet is intended to assist EOCs in determining their current network cybersecurity and resiliency capabilities and identify ways to improve their ability to defend against cyber incidents. The fact sheet can be accessed here: https://www.cisa.gov/sites/default/files/video/22_0307_ecd_Cyber_Resiliency_Resources_for_Public_Safety_Factsheet_508c.pdf.

- SAFECOM Emergency Communications Center (ECC) Cybersecurity Resources: Includes the Cyber Risks to Next Generation 911 (NG911) document which provides sample risk reduction strategies, actions, and educational and training resources. The NG911 document can be found here: https://www.cisa.gov/publication/next-generation-911. In addition, the National 911 Program Office also hosts Cybersecurity Resources. Access these resources at https://www.cisa.gov/safecom/resources.

EOC Management

This section discusses functions and considerations for supporting and sustaining EOC operations.

1. Standard Operating Procedures

As part of the planning process, leaders should develop and distribute standard EOC operating procedures to all concerned. Procedures should describe EOC layout and functions, the duties of major teams and individuals and the use of EOC displays, message forms and other operational forms. Standard operating procedures can rely on FEMA guidance regarding EOC operations, organization and staffing—including recommendations on wall displays, staff and individual functions, message flow and forms, and other operational procedures.

During a developing emergency, EOC activation may become necessary. EOC standard operating procedures clearly outline simple processes for opening the EOC, including the following elements:

- Authority;
- Elected officials, senior leaders, and tribal representatives;
- Conditions for activation;
- Notice events;
- Notifications;
- Setup;
- Deactivation;
- Annual review; and
- Testing and exercising activation procedures.

1.1. Authority

Standard operating procedures should list at least three officials—by title, not name—with the authority to activate the facility and call in EOC staff. Procedures should also include any special considerations for the activation of hybrid or virtual emergency operations.

1.2. Elected Officials, Senior Leaders, and Tribal Representatives

FEMA's National Integration Center (NIC) has developed several resources focused on EOCs, all based on feedback and technical assistance requests. One such resource, the Senior Leader Toolkit, includes the Elected Official/Senior Leader Quick Reference Guide. This guide contains:

- Overarching priorities that apply to every incident;
- Essential responsibilities of senior executives;
- What to expect; and
- Public messaging examples.

Intentionally broad, the guide applies to diverse organizations across the nation. FEMA recommends that emergency managers customize the reference guide by including organizational points of contact (POCs) and relevant operational details, such as how often the EOC will provide situation reports. Emergency managers should review the customized reference guide with their leadership before an incident occurs. To view the Senior Leader Toolkit, visit https://www.fema.gov/emergency-managers/nims/components/senior-leader-toolkit.

Virtual environments may allow for greater flexibility when engaging elected officials, senior leaders, and tribal representatives. Dashboards, situational awareness reports and other information sources can be tailored to specifics roles and organizations, allowing for an always updating view-only stream.

1.3. Conditions for Activation

Standard operating procedures or other documents should clearly address questions such as these: Under what conditions should the EOC be activated? To what level of activation? What determines the type of EOC activated (virtual, hybrid or in person)? Can authorized individuals activate the EOC and emergency staff for a surprise emergency exercise?

Conditions for activation may differ in a hybrid or virtual environment. It should be expected that activations become more common when hybrid or virtual environments can provide “hot EOC” capabilities 24/7. Determining if specific events necessitate one option over another, reexamining activation thresholds and exploring the ability to support neighboring or even distant jurisdictions virtually are important differences in hybrid and virtual environments. Decision trees and pre-determined criteria can assist jurisdictions in routinizing their activation processes across physical, hybrid and virtual environments. Criteria should also be established for individual stakeholders on when to discontinue virtual emergency operations and relocate to an office or physical EOC. Some of these criteria could include unsafe working conditions, long-duration power outages, internet outages, etc.

1.4. Notice Events

EOCs often become involved in planned activities such as inaugurations, parades, demonstrations, fairs, sporting events, etc. The EOC activates merely in anticipation of a potential incident, not in response to one. To be clear, EOCs can be activated for both events (planned and scheduled) and incidents (unplanned and unscheduled). Staff members should account for known risks and threats and establish policies and procedures that can adapt as necessary to changing requirements. Hybrid

and virtual EOC activations may be an effective way to initiate preparedness coordination across all stakeholders in an expected long-duration incident, gradually shifting to an in-person activation as conditions warrant and if a physical EOC is established. This process can reduce fatigue and toil across key stakeholders before the incident has even scaled up.

1.5. Notifications

Standard operating procedures should include a notification contact list of all crisis management team members, including work, home and other phone numbers at which they can be reached, as well as virtual communication methods such as email or chat applications. This list should be created during steady-state and updated regularly. Additionally, the primary method of communication should be predetermined and tested.

The list should also designate which agencies inside and outside the jurisdiction leaders should notify in an emergency, depending on the nature of the incident. Jurisdictions may consider using a high-speed notification system to notify staff about activation. Furthermore, links to the applicable location within crisis information management system or collaboration suites can be embedded directly in the notification, giving stakeholders “one-click” access to link up with their peers.

1.6. Setup

If the EOC is not a 24-hour facility, the standard operating procedures should specify how to set up the Ops Room and who is responsible for various setup tasks. At minimum, documentation should include the following:

- Keys: Who (by title) has them, or where are they located? How are software passwords safely shared and updated?;
- Furniture: Where is it stored and where does it go? Who is responsible for furniture setup, and how will they receive the alert? Include an EOC floor plan;
- Communications: If the EOC does not have permanently installed communications devices (phone sets, government radio transceivers, intercom systems, commercial radios, television receivers, scanners, etc.), where are they stored? Where do they belong in the EOC? Who is responsible for communications setup, and how will they receive the alert? Again, a floor plan is necessary;
- Display devices: If the EOC does not have mounted display devices, where are they stored and where do they belong upon EOC activation? Who is responsible for these devices?; and
- Equipment and supplies: Where are the copy machines, typewriters, calculators, cameras, maps, grease pencils, whiteboard, erasers, forms, staplers, staple removers, pens, pencils, paper and other supplies stored, and who is responsible for bringing them to the EOC?

Virtual activations: Who manages the virtual platform and licenses? Do any incident-specific chat channels need to be configured? Do any video calls need to be scheduled? Do any files or pages need to be added or reconfigured on the crisis information management system? Do employees take laptops home with them daily for continuity of operations in the event the EOC is unreachable?

1.7. Deactivation

It is rare that EOCs deactivate all at once. The best deactivation method scales back functions over time, as resources become unnecessary. Standard operating procedures should detail the deactivation process: Who determines when an operation can deactivate, and who is responsible for cleanup and replenishing expendables?

Deactivation should include after-action reports, which are valuable in communicating operational deficiencies and lessons learned to state, federal and cooperating agencies and jurisdictions.

Similar to the possible use of virtual emergency operations in the process of scaling up a physical EOC, deactivation of physical EOCs may also initiate an increase in hybrid or virtual activities for the remainder of the incident to reduce fatigue and toil. While all organizations may eventually discontinue their use of a virtual system, many others may continue to use the services for months into recovery. This situation may be another reason to consider the use of existing and familiar collaboration platforms to manage crisis information within an organization.

1.8. Annual Review

EOCs should review their standard operating procedures annually to ensure consistency with current plans, procedures, equipment, recordkeeping systems, display devices and communications capabilities. Contact lists also require regular updating. After leaders update the procedures, they can schedule supplementary training sessions or exercises, in addition to regularly scheduled exercises, to reinforce changes in the operating procedures.

1.9. Testing and Exercising Activation Procedures

Like any aspect of emergency operations, leaders should test EOC activation, setup, and deactivation procedures using drills or training sessions. Leaders can then modify the procedures to fit the jurisdiction's needs and the changing capabilities of the EOC staff and emergency equipment. See the Planning, Training and Exercises section of this document, below, for more details.

Hybrid and virtual procedures should be tested as realistically as possible, with opportunities for stakeholders to attempt connecting to crisis information management systems using the locations and devices that they may find themselves in during an emergency. In addition, efforts should be made to conduct hybrid and virtual exercises after hours and/or weekends to uncover potential challenges with activating emergency operations outside of normal business hours.

Planning, Training and Exercises

1. Planning

Planners are responsible for coordinating and developing plans that are flexible, actionable, and guide operations to accomplish a mission. EOCs perform two types of planning: deliberate planning and incident action planning.

Effective planning ensures that the whole community is represented and involved in the planning process. The most realistic and complete plans are prepared by a diverse planning team, including representatives from the jurisdiction's departments and agencies, civic leaders, businesses and organizations (civic, social, faith-based, humanitarian, educational, advocacy, professional) who are able to contribute critical perspectives or have a role in executing the plan.

1.1. The Preparedness Cycle

Planning, especially in the EOC context, includes the collection, evaluation and dissemination of operational information related to an incident. The Planning section maintains information on the current situation, the forecast and the status of resources assigned to the incident.

Through the use of EOC Skillsets personnel can be trained and qualified to perform the following Planning Tasks in an EOC:

- Reference pre-incident plans;
- Develop and write EOC action plans and other incident-specific plans;
- Disseminate plans; and
- Facilitate the ongoing planning process.

Planning is one of the key components of the preparedness cycle. The preparedness cycle (Figure 4) illustrates the way leaders continuously evaluate and improve their plans through a cycle of planning, organizing, equipping, training, exercising, evaluating and taking corrective action.

Figure 4. The Preparedness Cycle

For more information on developing and maintaining the EOP and general planning, visit https://www.fema.gov/sites/default/files/2020-07/developing-maintaining-emergency-operations-plans.pdf.

1.2. Incident Action Planning

The incident action planning process and IAPs (Incident Action Plans) are central to managing incidents. IAPs help synchronize operations and ensure that operations support incident objectives. Using a disciplined system of planning phases and meetings fosters collaboration/partnerships and keeps incident operations focused. The incident action planning process has the following phases:

- Understand the situation;
- Establish incident objectives;
- Develop the plan;
- Prepare and disseminate the plan; and
- Execute, evaluate and revise the plan.

For more information and guidance on incident action planning, see the References and Resources section of this document, below, and visit https://training.fema.gov/emiweb/is/icsresource/assets/incident%20action%20planning%20process.pdf.

2. NIMS Training and EOCs

NIMS provides principles, structures and processes that link the nation's responders together, enabling them to meet challenges that are beyond the capacity of any single jurisdiction or organization. The effectiveness of NIMS hinges on how well incident personnel at all levels understand their roles and responsibilities. Training is critical to building a common understanding and ensuring that responders apply NIMS concepts across SLTT jurisdictions, as well as partner organizations. NIMS training is one piece of a comprehensive incident management program involving a continuous cycle of planning, organizing, equipping, training, exercising, evaluating and taking corrective action.

The NIMS Training Program outlines a path for developing and maintaining NIMS and provides guidance for EOCs in developing their training plans. To see the full NIMS Training Program, visit https://www.fema.gov/nims-training.

2.1. EOC Training Progression

The NIMS Training Program recommends that EOC staff follow the EOC training progression. Each Authority Having Jurisdiction (AHJ) determines how far individuals need to progress based on their role within the EOC and the size and complexity of incidents they will support. See Figure 5 for details.

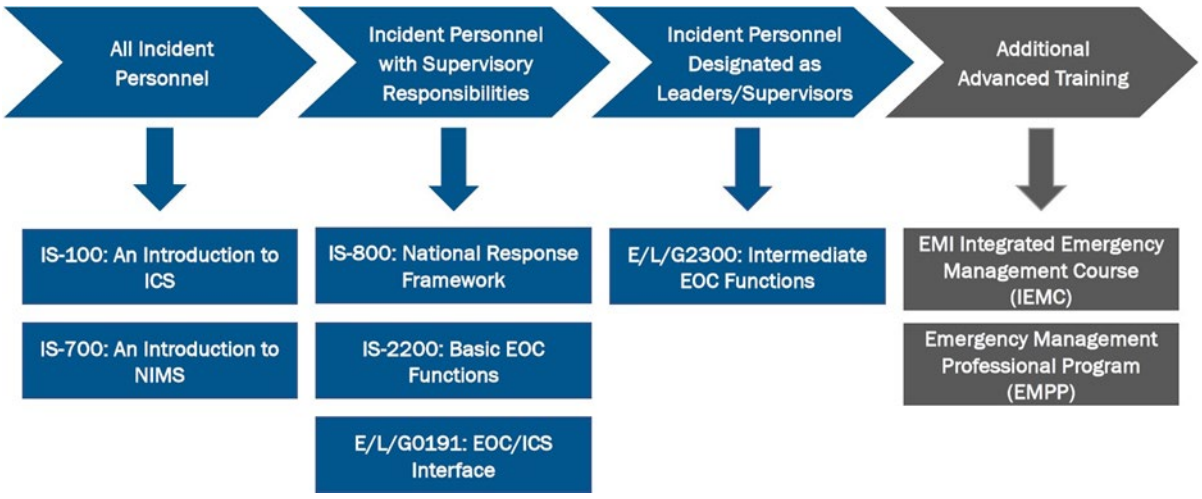

Figure 5. EOC Training Progression

In an EOC environment, just-in-time training (JITT) provides essential administrative, functional and operational information for those serving in various EOC roles. JITT is supplemental to ICS training and other advanced training. See the box below for details.

Just-in-Time Training in EOCs

JITT typically provides trainees with specific, readily-available information right when they need it. It answers questions such as:

- What information, tools and assistance, if applicable, are required to do my tasks?
- How do I execute the required processes in the EOC?
- What tasks come next for my assigned job?

Other critical EOC elements covered in JITT methods include:

- Check-in/check-out process
- How the EOC functions
- Safety
- EOC layout
- Workstations
- Job assignment
- Media and public relations
- Situation updates and operational periods

All EOC Personnel: All incident personnel working within an EOC should complete the following courses for foundational knowledge of incident response:

- IS-100[9]: Introduction to the Incident Command System, ICS-100 – This course introduces ICS and provides the foundation for higher-level ICS training; and
- IS-700: National Incident Management System, An Introduction – This course introduces NIMS concepts and principles.

EOC Personnel with Leadership Responsibilities: Supervisory personnel working within an EOC should complete the following courses for additional background in incident management systems with leadership responsibilities:

- IS-800: National Response Framework, An Introduction – This course introduces participants to the concepts and principles of the National Response Framework (NRF);

[9] *Note:* Many FEMA Emergency Management Institute courses use alpha identifiers and numbers in the course title (for example, IS-100C: Introduction to the Incident Command System, ICS-100). The alpha identifier at the end (in this example, C) typically indicates the version of the course—the higher the letter, the more recent the course.

- IS-2200: Basic EOC Functions – This course prepares incident personnel working in an EOC to understand the role and functions of an EOC during incident response and the transition to recovery;
    - FEMA recommends that personnel with leadership responsibilities in an EOC complete IS-2200 instead of IS-200.
- E/G/L 0191: Emergency Operations Center/Incident Command System Interface – This course reviews ICS and EOC responsibilities and functions.

EOC Personnel Designated as Leaders/Supervisors: EOC leaders need enhanced knowledge. This course applies higher-level concepts, methods and tools for larger, more complex incidents:

- E/G/L 2300: Intermediate EOC Functions – This course describes the role, design and function of EOCs as components of a MACS.

EOC Advanced Training: This training is above and beyond what is necessary for FEMA preparedness grant eligibility. Students participating in these advanced courses will broaden their understanding of emergency management concepts:

- Emergency Management Institute (EMI) Integrated Emergency Management Course (IEMC) – This is an exercise-based training series for EOC personnel; and
- FEMA's Emergency Management Professional Program (EMPP) – This program includes three academies: Basic, Advanced and Executive.

3. Exercises and EOCs

Conducting exercises is an integral part of the preparedness cycle. Exercises provide leaders with an opportunity to shape planning, assess/validate capabilities and identify strengths and areas for improvement. The Homeland Security Exercise and Evaluation Program[10] (HSEEP) provides a set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design/development, conduct, evaluation and improvement planning. This section covers exercise concepts.

3.1. HSEEP Principles

HSEEP is the cornerstone of the nation's guidance for exercise design, development and evaluation. HSEEP is flexible, scalable, adaptable and designed for use by stakeholders across the whole community. Nationwide use of HSEEP supports a consistent approach to exercises and measuring

[10] For more information about HSEEP, visit https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

progress toward building, sustaining and delivering core capabilities. The fundamental principles of HSEEP, detailed below, align and support the NIMS guiding principles:

- Driven by senior leader guidance;
- Informed by risk;
- Capability-based and objective-driven;
- Follows a progressive exercise planning approach;
- Encourages whole community integration; and
- Uses a common methodology.

3.2. Exercise Types

The type of exercise selected will depend on the specific objectives, goals, resources and needs of the jurisdiction planning the exercise. HSEEP has two broad categories of exercises—discussion-based and operations-based—which together encompass seven exercise types:

Discussion-based exercises:

- Seminars: familiarize players with current plans, policies, agreements and procedures;
- Workshops: achieve a specific goal or build a product (for example, standard operating procedures, policies or plans);
- Tabletop exercises: help participants understand and assess plans, policies, procedures and concepts; and
- Games: explore decision-making processes and examine the consequences of decisions.

Operations-based exercises (the higher level of the exercise program):

- Drills: test a single operation or function;
- Functional exercises: test and evaluate capabilities, functions, plans and staffs in real time; movement of resources is usually simulated; and
- Full-scale exercises: typically, the most complex and resource-intensive; implement and analyze plans, policies, procedures and cooperative agreements; usually include real-time movement of resources.

Facility drills are training activities aimed at perfecting facility functions and skills. The drills help staff members become proficient in their emergency functions through repetitive practice. They are

usually short in duration. Trainers can either announce them ahead of time or execute them as a surprise to test capability and proficiency.

Hybrid and virtual environments warrant separate drills to help build proficiency. An example of a drill focused on virtual emergency operations would be a monthly test for all stakeholders accessing the crisis information management system(s) from their mobile devices at home.

3.3. Equipment Checks

Regular mechanical and equipment checks are another integral part of every EOC plan. All of the following require regular checks for reliability and operability:

- Emergency systems, lighting, backup power, audio/visual equipment and communications;
- Battery-powered equipment, from portable radios to handheld calculators; and
- All computers serving the EOC (test hardware, update software).

Ultimately, if an EOC is to respond to a variety of crises, it must be prepared to react with current data, functioning equipment and trained personnel. If any of these key elements fails, the EOC may not be able to serve the jurisdiction it intends to protect.

3.4. Evaluation and Improvement

Planning and conducting exercises are important phases in EOC preparation. However, through exercise evaluation, jurisdictions assess the capabilities necessary to accomplish a mission, function or objective. Evaluation connects the exercises to the Evaluate/Improve phase of the preparedness cycle (Figure 4).

The communication of accurate, timely exercise evaluation results is crucial and typically takes place through the development of the after-action report and improvement planning process. The resulting document includes an exercise overview, a capabilities analysis and a list of corrective actions. Leaders should track these corrective actions and continually report on them until their completion. These efforts are part of a comprehensive continuous improvement process that applies before, during and after an exercise.

Resource Management During an Incident

Managing resources during an incident involves standard methods to identify, order, mobilize and track resources. Sometimes, the identification and ordering process compresses, such as when an Incident Commander (IC) identifies the resources necessary for a given task and orders them directly. However, in larger, more complex incidents, the IC relies on the resource management process and ICS/EOC personnel to identify and meet resource needs. Figure 6 shows the six main tasks involved in resource management during an incident.

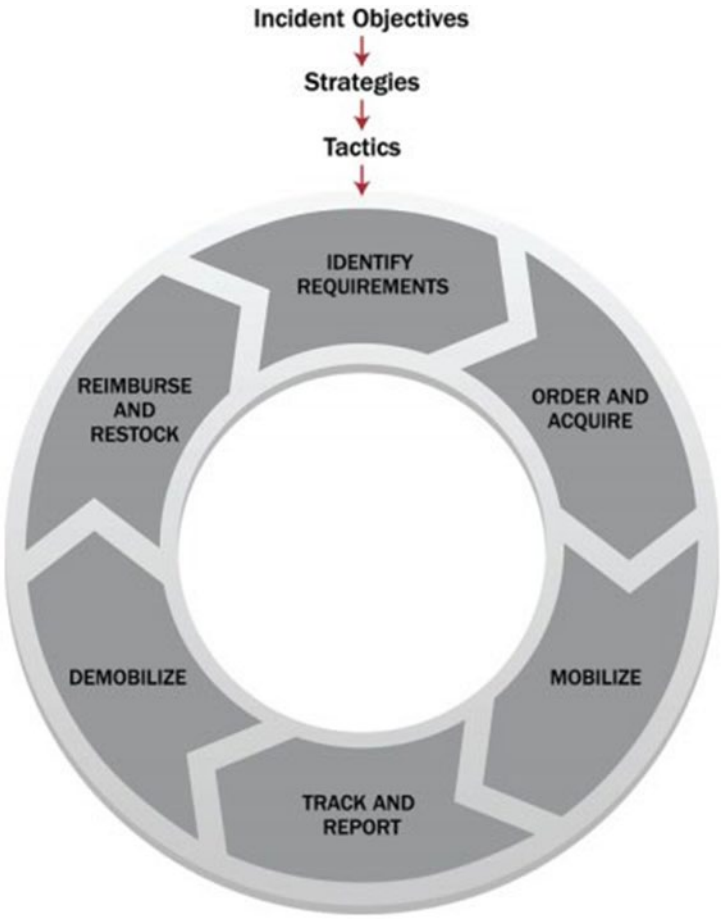

Figure 6: Resource Management Process

1.1. Identifying Requirements

During an incident, field and EOC personnel continually identify, validate and refine resource needs. This ongoing process involves identifying the type and quantity of necessary resources, the shipping address for resources and who will receive and use the resources.

Resource availability and needs constantly change as an incident evolves. Consequently, incident management personnel and their affiliated organizations should coordinate as closely and as early as possible, both before and during incidents.

2. Ordering and Acquiring

Incident and EOC staff make initial and ongoing assessments of resource requirements and either activate or request those resources. Incident personnel can order additional resources by executing contracts, implementing mutual aid agreements or requesting assistance from another level of government (for example, from local government to state, or from a state to the federal government). To facilitate reimbursement and prevent duplication, EOCs should understand and follow appropriate authorities and processes for ordering and acquiring resources.

Incident and EOC personnel request resources based on incident priorities and objectives. They base decisions about resource allocation on jurisdictional or organizational protocol (for example, minimum staffing levels) and, when applicable, on the resource demands of other incidents. The organization providing resources consents to the request and communicates any discrepancies between requested resources and those available for delivery.

2.1. Resource Requests

Organizations requesting resources should provide enough detail that those receiving the request will understand what is necessary. Using NIMS resource names and types helps ensure clear communication. Requestors should include the following information in a request:

- Detailed item description, including quantity, kind and type (if known) or a description of required capability and its intended use;
- Suitable substitute resources and preferred sources, if they exist;
- Detailed specifications for uncommon or nonstandard incident resources;
- Required arrival date and time;
- Required delivery or reporting location;
- Position title of the individual to whom the resource should report, if applicable; and
- Any incident-specific health or safety concerns (for example, vaccinations, adverse living/working conditions or identified environmental hazards).

Personnel receive assignments based on their qualifications and the incident's needs, as well as on jurisdictional licensing requirements or limitations. Personnel in some fields, including law enforcement and medicine, have limited authority outside the jurisdiction in which they are sworn or licensed.

Published by the NIC, the Resource Typing Library Tool (RTLT) is FEMA's online catalog of national resource typing definitions, position qualifications and PTBs. For more information about this tool, visit https://rtlt.preptoolkit.fema.gov/Public/Home/Help.

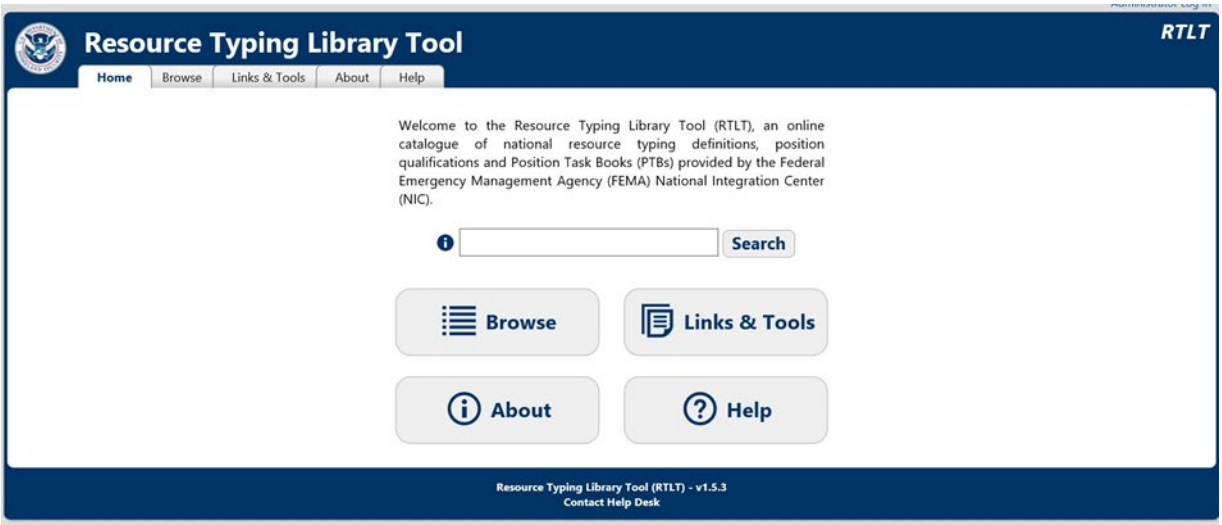

Figure 7: Resource Typing Library Tool

2.2. Incident Assignments

Safe, effective incident management depends on all personnel executing their responsibilities according to established guidelines. Personnel deploy to incidents at the request of the appropriate authority. Individuals remain deployment-ready by maintaining the skills, knowledge, certifications, physical fitness, equipment and other elements that FEMA requires or recommends for their position.

As part of a comprehensive orientation program for deployed resources, EOCs may consider developing a welcome kit—perhaps part of a JITT packet—containing information for on-site and off-site readiness. Items include an area/facility map, key phone numbers (including Liaison Officer phone numbers), Wi-Fi password/instructions, links to the IAP, etc.

Abbreviations

ADA	Americans with Disabilities Act
AFN	Access and Functional Needs
AHJ	Authority Having Jurisdiction
BEOC	Business Emergency Operations Center
CBRN	Chemical, Biological, Radiological and Nuclear
CDC	Centers for Disease Control and Prevention
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations
CRIA	Community Resilience Indicator Analysis
DHS	Department of Homeland Security
DOC	Department Operations Center
DRRA	Disaster Recovery Reform Act
DVN	Digital Volunteer Network
ECC	Emergency Communications Center
EEI	Essential Elements of Information
EMAC	Emergency Management Assistance Compact
EMI	Emergency Management Institute
EMPP	Emergency Management Professional Program
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EPA	Environmental Protection Agency

ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
GIS	Geographic Information Systems
HAZMAT	Hazardous Materials
HSEEP	Homeland Security Exercise and Evaluation Program
HVAC	Heating, Ventilation and Air Conditioning
IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IEMC	Integrated Emergency Management Course
IMAT	Incident Management Assistance Team
IMT	Incident Management Team
ISP	Internet Service Provider
IT	Information Technology
JFO	Joint Field Office
JIC	Joint Information Center
JIS	Joint Information System
JITT	Just-In-Time Training
LAN	Local Area Network
LTE	Long-term Evolution
MAC Group	Multiagency Coordination Group
MACS	Multiagency Coordination System
MRE	Meals Ready to Eat

NBEOC	National Business Emergency Operations Center
NCPIP	National Continuity Policy Implementation Plan
NDRF	National Disaster Recovery Framework
NG911	Next Generation 911
NGO	Nongovernmental Organization
NIC	National Integration Center
NIMS	National Incident Management System
NPF	National Planning Frameworks
NPG	National Preparedness Goal
NQS	National Qualification System
NRCC	National Response Coordination Center
NRF	National Response Framework
NTED	National Training and Education Division
Ops Room	Operations Room
PIO	Public Information Officer
PMEF	Primary Mission Essential Functions
POC	Point of Contact
PPE	Personal Protective Equipment
PSC	Planning Section Chief
PTB	Position Task Book
RAPT	Resilience Analysis and Planning Tool
ROC	Regional Operations Center
RoIP	Radio over Internet Protocol
RSF	Recovery Support Function

RTLT	Resource Typing Library Tool
SaaS	Software as a Service
SLTT	State, Local, Tribal and Territorial
SMS	Short Message Service
THIRA	Threat and Hazard Identification and Risk Assessment
UPS	Uninterruptable Power Supply
USNG	United States National Grid
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Glossary

For the purpose of National Incident Management System (NIMS) and Emergency Operation Centers (EOCs), the following terms and definitions apply:

Access and Functional Needs (AFN): Individual circumstances requiring assistance, accommodation or modification for mobility, communication, transportation, safety, health maintenance, etc., due to any temporary or permanent situation that limits the ability of an individual (such as a person with disabilities) to act in an emergency.

Agency: A government element with a specific function offering a particular kind of assistance.

Agency Administrator/Executive: The official responsible for administering policy for an agency or jurisdiction.

Agency Representative: A person whose agency or organization (a primary, assisting or cooperating state, local, tribal and territorial (SLTT) or federal government agency; a non-governmental organization (NGO); or a private organization) has the authority to make decisions affecting the agency or organization's participation in incident management activities, in consultation with the organization's leadership.

Americans with Disabilities Act (ADA): A civil rights law that prohibits discrimination against individuals with disabilities in all areas of public life, including jobs, schools, transportation and all public and private places that are open to the general public. The purpose of this law is to make sure that people with disabilities have the same rights and opportunities. The ADA gives civil rights protections to individuals with disabilities similar to those provided to individuals on the basis of race, color, sex, national origin, age and religion. It guarantees equal opportunity for individuals with disabilities in public accommodations, employment, transportation, state and local government services and telecommunications.

Area Command: An organization that oversees the management of multiple incidents or oversees the management of a large or evolving situation with multiple Incident Command System (ICS) organizations. See Unified Area Command.

Assigned Resource: A resource that has checked in and received work assignments for an incident.

Assignment: A task given to a person or team to perform based on operational objectives defined in the Incident Action Plan (IAP).

Assistant: A title for subordinates of principal Command Staff and subordinates of EOC executive staff. The title indicates a level of technical capability, qualification and responsibility subordinate to the primary positions. Unit leaders may also have assistants.

Assisting Agency: An agency or organization providing personnel, services or other resources to the agency with direct responsibility for incident management.

Authority Having Jurisdiction (AHJ): An entity that has the authority and responsibility for developing, implementing, maintaining and overseeing the personnel qualification process within its organization or jurisdiction. The AHJ may be a state or federal agency, training commission, NGO, private sector company or a tribal or local agency such as a police, fire or public works department. In some cases, the AHJ may provide support to multiple disciplines that collaborate as part of a team, such as an Incident Management Team (IMT).

Available Resource: A resource that is checked in and available for assignment on an incident.

Badging: Assigning physical, incident-specific credentials to establish legitimacy and permit access to incident sites. See credentialing.

Base: See incident base.

Branch: The 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. The Federal Emergency Management Agency (FEMA) uses Roman numerals or functional areas to identify branches.

Camp: A geographical site within the general incident area (separate from the incident base) that has the equipment and staff to provide sleeping accommodations, food, water and sanitary services to incident personnel.

Certification: The process of authoritatively attesting when individuals meet qualifications established for key incident management functions and are, therefore, qualified for specific positions.

Chain of Command: The orderly line of authority within the ranks of incident management organizations.

Check-In: The process by which resources first report to an incident. All responders, regardless of agency affiliation, report in to receive an assignment in accordance with the Incident Command (IC) or Unified Command's established procedures.

Chief: The ICS title for individuals responsible for managing functional sections: Operations, Planning, Logistics and Finance/Administration.

Clear Text: Communication that does not use codes. See plain language.

Command: The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority.

Command Staff: A group of incident personnel that the IC or Unified Command assigns to support the command function at an Incident Command Post (ICP). Command Staff often include a Public Information Officer (PIO), a Safety Officer, a Liaison Officer and any assistants they may have. Additional positions may be necessary, depending on the incident.

Community Resilience Indicator Analysis (CRIA): A federal analysis of peer-reviewed research on community resilience challenges in U.S. counties.

Continuity of Operations (COOP): As defined in the National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20), COOP is an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions continue to occur during a wide range of emergencies, including localized acts of nature, accidents and technological or attack- related emergencies.

Cooperating Agency: An agency supplying assistance other than direct operational or support functions or resources to the incident management effort.

Coordinate: To exchange information systematically among principals who may need certain types of information to carry out specific incident management responsibilities.

Core Capability: An element defined in the National Preparedness Goal (NPG) as necessary to prevent, protect against, mitigate, respond to and recover from the threats and hazards that pose the greatest risk.

Credentialing: Providing documentation that identifies personnel and authenticates and verifies their qualification for a particular position. See badging.

Critical Infrastructure: Assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Data: The rawest form of information, which can include numbers, characters, symbols, or words, that have not yet been placed into context or evaluated against other data and information. Data may come from a wide variety of inputs, including operational federal and non-federal assets, eyewitness reports, field observations, social media, and weather reports.

Delegation of Authority: A statement that the agency executive delegating authority and assigning responsibility provides to the IC. The Delegation of Authority can include priorities, expectations, constraints and other considerations or guidelines, as necessary.

Demobilization: The orderly, safe and efficient return of an incident resource to its original location and status.

Department Operations Center (DOC): An operations or coordination center dedicated to a single, specific department or agency. A DOC focuses on internal agency incident management and response. DOCs are often linked to a combined agency EOC, with an authorized agent (or agents) representing the department or agency.

Deputy: A fully qualified individual who, in the absence of a superior, can be delegated the authority to manage a functional operation or to perform a specific task. In some cases, a deputy can act as relief for a superior and, therefore, should be fully qualified in the position. Deputies can be assigned to the IC, EOC director, General Staff and branch directors.

Digital Volunteer Network (DVN): A collection of volunteers who support emergency management efforts during disasters by curating, analyzing and creating visualizations of crowdsourced data (data collected from large groups of people who submit information/responses via websites, social media and smartphone apps).

Director: The ICS title for an individual responsible for supervising a branch. Also, an organizational title for an individual responsible for managing and directing the team in an EOC.

Disaster Recovery Reform Act (DRRA): Part of the Federal Aviation Administration Reauthorization Act of 2018. The DRRA aims to improve FEMA's disaster preparedness, response, recovery and mitigation programs and build the nation's capacity for future catastrophic events.

Dispatch: The ordered movement of a resource or resources to an assigned operational mission, or an administrative move from one location to another.

Division: The organizational level having responsibility for operations within a defined geographic area. Divisions are established when the number of resources exceeds the manageable span of control of the Section Chief. See group.

Emergency: Any incident, whether natural, technological or human caused, that necessitates responsive action to protect life or property.

Emergency Management Assistance Compact (EMAC): A congressionally ratified agreement that provides form and structure to interstate mutual aid. Through EMAC, a disaster-affected state can request and receive assistance from other member states quickly and efficiently, resolving two key issues up front: liability and reimbursement.

Emergency Management Institute (EMI): FEMA's national focal point for the development and delivery of emergency management training to enhance the capabilities of officials from SLTT governments and volunteer organizations.

Emergency Management Professional Program (EMPP): A structured and progressive framework to help emergency managers acquire the knowledge, skills and abilities to enter and progress through the field and to meet the challenges of a dynamic and complex environment. The EMPP curriculum is designed to provide a lifetime of learning for a career in emergency management.

Emergency Operations Center (EOC): The physical location where the coordination of information and resources to support incident management (on-scene operations) normally takes place. An EOC may be housed in a temporary facility or in a permanently established, central facility, or a building that houses another government agency within the jurisdiction. A virtual EOC is an exception to a physical EOC.

Emergency Operations Plan (EOP): A plan for responding to a variety of potential hazards.

Emergency Support Functions (ESF): An organized grouping of the governmental, private sector and NGO capabilities and services that are most likely to be necessary for managing domestic incidents.

Environmental Protection Agency (EPA): An agency of the United States government whose mission is to protect human and environmental health and is responsible for creating standards and laws promoting the health of individuals and the environment. The agency is headquartered in Washington, D.C.

Essential Elements of Information (EEI): Important and standard information items supporting timely and informed decisions.

Evacuation: The organized, phased and supervised withdrawal, dispersal or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

Event: See planned event.

Federal: Of or pertaining to the federal government of the United States.

Finance/Administration Section: The ICS section responsible for an incident's administrative and financial considerations.

Fusion Center: State-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners.

General Staff: A group of incident personnel organized according to function and reporting to the IC or Unified Command. The ICS General Staff consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief and Finance/Administration Section Chief.

Geographic Information Systems (GIS): A framework for gathering, managing and analyzing data rooted in the science of geography. GIS analyzes spatial location and organizes layers of information into visualizations such as maps and 3D scenes, providing deeper insights into patterns, relationships and situations.

Group: An organizational subdivision established to divide the incident management structure into functional areas of operation. Groups are composed of resources assembled to perform a special function not necessarily within a single geographic area. See division.

Hazard: Something potentially dangerous or harmful; often the root cause of an unwanted outcome.

Homeland Security Exercise and Evaluation Program (HSEEP): A set of guiding principles for exercise programs, as well as a common approach to exercise program management, design, development, conduct, evaluation and improvement planning.

Incident: An occurrence, natural or human caused, that necessitates a response to protect life or property. In this document, incident includes planned events as well as emergencies and disasters of all kinds and sizes.

Incident Action Plan (IAP): An oral or written plan containing the IC's or Unified Command's objectives and addressing tactics and support activities for the planned operational period, typically 12 to 24 hours.

Incident Base: A location where personnel coordinate and administer logistics functions for an incident. There is typically only one base per incident. The ICP may be co-located with the incident base.

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

Incident Commander (IC): The individual responsible for on-scene incident activities, including developing incident objectives and ordering and releasing resources. The IC has overall authority and responsibility for conducting incident operations.

Incident Command Post (ICP): The field location where staff perform the primary functions of incident command. The ICP may be co-located with the incident base or other incident facilities.

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 work. ICS brings procedures, personnel, facilities, equipment and communications into a common organizational structure to aid in the management of on-scene resources during incidents. ICS applies to small, large and complex incidents of all kinds, including planned events.

Incident Management: The broad spectrum of activities and organizations providing operations, coordination and support at all levels of government, using both governmental and nongovernmental resources to plan for, respond to and recover from an incident, regardless of cause, size or complexity.

Incident Management Assistance Team (IMAT): A team of ICS-qualified personnel, configured according to ICS, that deploy in support of affected jurisdictions and on-scene personnel.

Incident Management Team (IMT): A rostered group of ICS-qualified personnel consisting of an IC, Command and General Staff, and personnel assigned to other key ICS positions.

Incident Objective: A statement of a desired incident outcome. Incident objectives drive strategies and tactics. Incident objectives should be realistic, achievable and measurable, yet flexible enough to allow strategic and tactical alternatives.

Incident Personnel: All individuals who have roles in incident management or support, whether on scene, in an EOC or in a Multiagency Coordination Group (MAC Group).

Information: Knowledge or data from a variety of federal and non-federal resources about a particular fact or circumstance that has been placed into a context and can be used to make decisions but has not been analyzed.

Information Management: The collection, organization and control of the structure, processing and delivery of information from one or more sources to one or more audiences who have a stake in that information.

Integrated Emergency Management Course (IEMC): A four-day, exercise-based training activity allowing EOC personnel to practice simulated, realistic crisis situations within a structured learning environment.

Intelligence: In NIMS, intelligence refers exclusively to threat-related information developed by law enforcement, medical surveillance, and other investigative organizations.

Intelligence/Investigations Function: The effort to determine the source or cause of an incident (for example, disease outbreak, fire, complex coordinated attack or cyber incident) to control its impact and help prevent the occurrence of similar incidents. In ICS, this function may belong to the Planning Section, Operations Section, Command Staff or General Staff (as a separate section) or to a combination of these entities.

Interoperability: The ability of systems, personnel and equipment to exchange functionality, data, information and services with other systems, personnel and equipment—among public and private agencies, departments and other organizations—in a manner enabling them to operate effectively together.

Joint Field Office (JFO): The primary federal incident management field structure. The JFO is a temporary federal facility that provides a central location for the coordination of SLTT and federal governments, private sector organizations and NGOs that have primary responsibility for response and recovery.

Joint Information Center (JIC): A facility in which personnel coordinate incident-related public information activities. The JIC serves as the central POC for all news media. PIOs from all participating agencies co-locate in, or coordinate virtually through, the JIC.

Joint Information System (JIS): A structure that integrates overarching incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely and complete information during crisis or incident operations.

Jurisdiction: Jurisdiction has two definitions depending on the context:

- A range or sphere of authority: Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (for example, SLTT or federal boundary lines) or functional (for example, law enforcement or public health).

- A political subdivision (for example, municipal, county, parish, state or federal) with the responsibility to ensure public safety, health and welfare within its legal authorities and geographic boundaries.

Just-In-Time Training (JITT): A training system that provides required knowledge and skills right when and where they are needed so that trainees can apply them immediately and avoid learning loss.

Kind: As applied to incident resources, a class or group of items or people of the same nature or character or classified together because they have common traits.

Leader: The ICS title for an individual who is responsible for supervising a unit, strike team, resource team or task force.

Liaison Officer: A member of the ICS Command Staff responsible for coordinating with representatives from cooperating and assisting agencies or organizations.

Lifelines: The most fundamental services in the community that, when stabilized, enable all other aspects of society to function.

Local Government: A public entity responsible for the security and welfare of a designated area as established by law. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council is incorporated as a nonprofit under state law), regional or interstate government entity, agency or instrumentality of a local government, tribe or authorized tribal entity (in Alaska, a Native Village or Alaska Regional Native Corporation), rural community, unincorporated town or village or other public entity.

Logistics: Processes and procedures for providing resources and other services to support incident management.

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

Management by Objectives: A management approach fundamental to NIMS that involves (1) establishing objectives (specific, measurable and realistic outcomes to be achieved), (2) identifying strategies, tactics and tasks designed to achieve the objectives, (3) performing the tactics and tasks, and measuring and documenting results and (4) taking corrective action to modify strategies, tactics and performance to achieve the objectives.

Manager: The individual within an ICS organizational unit who has specific managerial responsibilities (for example, Staging Area Manager or Camp Manager).

Meals Ready to Eat (MRE): Self-contained, shelf-stable meals used as the main operational food ration, providing adequate nutrition during combat or field work for the U.S. armed forces.

Mission Area: One of five preparedness areas (prevention, protection, mitigation, response and recovery) designated in the NPG for grouping core capabilities.

Mitigation: The capabilities necessary to reduce the loss of life and property by lessening the impacts of natural and human-caused disasters, incidents and events.

Mobilization: Processes and procedures for activating, assembling and transporting resources that have been requested to respond to or support an incident.

Multiagency Coordination Group (MAC Group): A group, typically consisting of agency administrators or organization executives or their designees, that provides policy guidance to incident personnel, supports resource prioritization and allocation, and enables decision-making among elected and appointed officials, senior executives from other organizations and those responsible for incident management.

Multiagency Coordination System (MACS): An overarching term for the NIMS Command and Coordination systems: ICS, EOC, MAC Group/Policy Group and JIS.

Mutual Aid Agreement or Assistance Agreement: A written or oral agreement between and among agencies/organizations and jurisdictions that provides a mechanism for quickly obtaining assistance in the form of personnel, equipment, materials and other associated services. The primary objective is to facilitate the rapid, short-term deployment of support prior to, during and after an incident.

National: Of a nationwide character, including the SLTT and federal aspects of governance and policy.

National Business Emergency Operations Center (NBEOC): FEMA's virtual clearinghouse for two-way information sharing between public and private sector/NGO stakeholders before, during and after disasters.

National Incident Management System (NIMS): A systematic, proactive approach for guiding all levels of government, NGOs 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, from daily occurrences to those requiring a coordinated federal response.

National Integration Center (NIC): The FEMA group that develops doctrine and tools to lead the whole-community implementation of the National Preparedness System and NIMS.

National Planning Frameworks (NPF): Guidance documents, one for each of the five preparedness mission areas, describing how the whole community works together to achieve the NPG. The frameworks foster a shared understanding of roles and responsibilities, from the firehouse to the White House, and clarify how the nation coordinates, shares information and works together to achieve a more secure and resilient nation.

National Preparedness: Planning, organizing, equipping, training and exercising to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to and recover from the threats that pose the greatest risk to national security.

National Preparedness Goal (NPG): Doctrine describing what it means for the whole community to be prepared for the types of incidents that pose the greatest threat to national security, including acts of terrorism, emergencies and disasters, regardless of cause. The goal reads, "A secure and resilient

Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to and recover from the threats and hazards that pose the greatest risk."

National Preparedness System: An organized process to achieve the NPG's stated goal of a secure and resilient nation.

National Qualification System (NQS): A foundational guideline for qualifying personnel resources within NIMS. The guideline establishes guidance and tools to help stakeholders develop processes for qualifying, certifying and credentialing deployable emergency personnel.

National Response Coordination Center (NRCC): A multiagency coordination center located at FEMA headquarters. Its staff coordinates the overall federal support for major disasters and emergencies, including catastrophic incidents and emergency management program implementation. The National Response Coordination Center (NRCC) also houses the NBEOC.

National Response Framework (NRF): A guide for the nation's response to all types of disasters and emergencies. It is built on NIMS concepts for aligning key roles and responsibilities. It includes the ESFs.

Nongovernmental Organization (NGO): A nonprofit group that is based on the interests of its members, individuals or institutions. An NGO is not created by a government, but it may work cooperatively with the government. Examples of NGOs include faith-based groups, relief agencies, organizations that support people with AFN and animal welfare organizations.

Normal Operations/Steady State: The activation level that describes routine monitoring of the jurisdictional situation, with no event or incident anticipated.

Officer: The ICS title for a Command Staff member authorized to make decisions and act related to his/her area of responsibility.

Operational Period: The time scheduled for executing a given set of operation actions, as the IAP specifies. Operational periods can vary in length but are typically 12 to 24 hours.

Operational Security: Implementing procedures and activities to protect sensitive or classified operations involving sources and methods of intelligence collection, investigative techniques, tactical actions, countersurveillance measures, counterintelligence methods, undercover officers, cooperating witnesses and informants.

Operations Room (Ops Room): A specific location in the EOC where displays, equipment and emergency functions reside.

Operations Section: The ICS section responsible for implementing tactical incident operations described in the IAP. The Operations Section may include subordinate branches, divisions and groups.

Organization: Any association or group of people with like objectives. Examples include government departments and agencies, NGOs and private sector entities.

Plain Language: Communication that the intended audience can understand and that meets the communicator's purpose. For NIMS, plain language refers to a communication style that avoids or limits the use of codes, abbreviations and jargon during incidents involving more than one agency.

Planned Event: A scheduled, non-emergency activity such as a sporting event, concert or parade.

Planning Meeting: A meeting held at any point before or during an incident to select strategies and tactics for incident control operations and to plan for service and support.

Planning Section: The ICS section collects, evaluates and disseminates operational information related to an incident and helps prepare and document the IAP. This section also maintains information on the current and forecasted situation and on the status of assigned resources.

Position Qualifications: The minimum criteria necessary for individuals to fill a specific position.

Position Task Book (PTB): A document identifying the competencies, behaviors and tasks that personnel should demonstrate to become qualified for a defined incident management or support position.

Prevention: The capabilities necessary to avoid, prevent or stop a threatened or actual act of terrorism. In national preparedness guidance, prevention refers to preventing imminent threats.

Private Sector: Organizations and individuals that are not part of a governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce and industry.

Protection: The capabilities necessary to secure the homeland against acts of terrorism and human-caused or natural disasters, incidents and events.

Protocol: A set of established guidelines for action (applying to individuals, teams, functions or capabilities) under various specified conditions.

Public Information: Processes, procedures and systems for communicating timely, accurate and accessible information on an incident's cause, size and current situation; resources committed; and other matters of general interest to the public, responders and additional stakeholders, whether directly or indirectly affected.

Public Information Officer (PIO): A member of the ICS Command Staff responsible for interfacing with the public, the media and other agencies that have incident-related information needs.

Recovery: The capabilities necessary to help communities affected by an incident recover effectively.

Recovery Plan: A plan to restore an incident-affected area or community.

Recovery Support Functions (RSF): Organizing structures for the key functional areas of assistance outlined in the National Disaster Recovery Framework that group capabilities of government, private sector and NGO partner organizations to promote effective recovery from disasters before and after disasters strike.

Reimbursement: A mechanism to recoup funds expended for incident-specific activities.

Resilience Analysis and Planning Tool (RAPT): A publicly available GIS web map that allows users to visualize and prioritize resilience, response and recovery strategies.

Resource Management: Systems for identifying available resources at all jurisdictional levels to enable timely, efficient and unimpeded access to resources necessary to prepare for, respond to or recover from an incident.

Resources: Personnel, equipment, teams, supplies and facilities available or potentially available for assignment to incident operations. NIMS describes resources by kind and type and uses them in operational support or supervisory capacities at an incident or at an EOC.

Resource Team: See strike team.

Resource Tracking: The process that all incident personnel and staff from associated organizations use to maintain information regarding the location and status of resources ordered for, deployed to or assigned to an incident.

Resource Typing Library Tool (RTLT): FEMA's online catalog of national resource typing definitions, position qualifications and PTBs.

Response: The capabilities necessary to save lives, protect property and the environment and meet basic human needs after an incident has occurred.

Safety Officer: In ICS, a member of the Command Staff responsible for monitoring incident operations and advising the IC or Unified Command on all matters relating to operational safety, including the health and safety of incident personnel. The Safety Officer modifies or stops the work of personnel to prevent unsafe acts.

Section: The ICS organizational element having responsibility for a major functional area of incident management (Operations, Planning, Logistics or Finance/Administration); capitalized when part of an official name.

Single Resource: An individual, a piece of equipment and its personnel complement, or a crew/team of individuals with an identified work supervisor that can support incident response.

Situation Report: Confirmed or verified information regarding the details of an incident.

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

Staging Area: A temporary location for available resources in which personnel, supplies and equipment await operational assignment.

Standard Operating Procedure: A reference document or operations manual that provides the purpose, authorities, duration and details for the preferred method of performing a single function or several interrelated functions in a uniform manner.

State: In this guide, it includes any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

Status Report: Any report (such as a spot report) that includes vital or time-sensitive information. Status reports are typically function-specific. They are less formal than situation reports and are not always issued on a specific schedule.

Strategy: The general course of action or direction to accomplish incident objectives.

Strike Team: A set number of resources of the same kind and type that have an established minimum number of personnel, common communications and a team leader; capitalized when part of an official name. In the law enforcement community, strike teams are called resource teams.

Supervisor: The ICS title for an individual responsible for a division or group.

System: Any combination of processes, facilities, equipment, personnel, procedures and communications integrated for a specific purpose.

Tactics: The deployment and directing of resources on an incident to accomplish the objectives.

Task Force: Any combination of resources of various kinds and types assembled to support a specific mission or operational need; capitalized when part of an official name.

Terrorism: Any activity involving an act (1) that is dangerous to human life or potentially destructive of critical infrastructure and is a violation of the criminal laws of the United States or of any state or other subdivision of the United States and (2) that appears to be intended to intimidate or coerce a civilian population, or to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination or kidnapping.

Threat: A natural or human-caused occurrence, an individual, an entity or an action having or indicating the potential to harm life, information, operations, property or the environment.

Threat and Hazard Identification and Risk Assessment (THIRA): A three-step risk assessment process that helps communities understand their risks and determine the level of capability they need to address those risks.

Tools: Instruments and capabilities that allow the professional performance of tasks, such as information systems, agreements, doctrine, capabilities and legislative authorities.

Tribal Nations: The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) uses the term "Indian tribal governments." The term 'Indian tribal government' means the governing body of any Indian or Alaska Native tribe, band, nation, pueblo, village, or community that the Secretary of the Interior acknowledges to exist as an Indian tribe under the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 479a et seq.).

Type: A NIMS resource classification that applies a metric to the capability of a specific kind of resource to designate it as a specific numbered class.

Unified Area Command: A version of command that applies when incidents under an Area Command are multijurisdictional. See Area Command.

Unified Command: An ICS command structure that applies when more than one agency has incident jurisdiction or when incidents cross political jurisdictions.

Uninterruptable Power Supply (UPS): A system that compensates for loss of power to service equipment for a limited period. UPS units include short-duration battery devices and standby generators for longer duration.

Unit: The organizational element with functional responsibility for a specific activity within the Planning, Logistics and Finance/Administration sections in ICS; capitalized when part of an official name.

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

United States National Grid (USNG): A point and area reference system that FEMA and other incident management organizations use as an accurate and expeditious alternative to latitude/longitude.

Unity of Command: A NIMS guiding principle stating that everyone involved in incident management reports to and takes direction from only one person.

Unity of Effort: A NIMS guiding principle that provides coordination through cooperation and common interests and does not interfere with federal department and agency supervisory, command or statutory authorities.

Voice over Internet Protocol (VoIP): A technology that enables voice calls using a broadband internet connection instead of an analog phone line.

Whole Community: A focus on enabling a wide range of players from the private and nonprofit sectors to participate in incident management activities to foster better coordination and working relationships. Stakeholders include NGOs, the general public and all levels of government.

References and Resources

The following resources can assist communities across the nation in establishing, operating and continuously improving Emergency Operation Centers (EOCs).

COVID-19 Pandemic Operational Guidance

- The Federal Emergency Management Agency's (FEMA's) COVID-19 Pandemic Operational Guidance: All Hazards Incident Response and Recovery provides actionable guidance for state, local, tribal and territorial (SLTT) officials to prepare for response and recovery operations amidst the COVID-19 pandemic. This document highlights how FEMA has adapted to operating in the COVID-19 pandemic environment, but to the greatest extent possible, the foundational emergency management concepts remain. Updated and pertinent information is also available at https://www.fema.gov/media-collection/covid-19-pandemic-operational-guidance-all-hazards

- https://www.fema.gov/sites/default/files/2020-07/fema-2020-hurricane-pandemic-plan_english.pdf

Cybersecurity

- The Cybersecurity and Infrastructure Security Agency (CISA) leads the nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and the American way of life.

- CISA Central

- Emergency Services Sector Cybersecurity Initiative

- Public Safety Cyber and Resiliency Toolkit

- SAFECOM Emergency Communications Center (ECC) Cybersecurity Resources

Emergency Support Function (ESF)

- The ESFs, part of the National Response Framework (NRF), provide the structure for coordinating federal interagency support for a federal response to an incident.

- https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response

FEMA National Training and Education Division (NTED)

- NTED develops and delivers training courses to prepare state and local first responders to prevent, protect, respond to and recover from catastrophic events.

- https://www.firstrespondertraining.gov/frts/npccatalog?catalog=EMI[11]

Incident Command System (ICS) Resource Center

- The ICS Resource Center, which the Emergency Management Institute (EMI) maintains, provides information about and links to an extensive array of ICS training materials, job aids, position checklists and forms.

- https://training.fema.gov/emiweb/is/icsresource/index.htm

Incident Action Planning Guidance

- The incident action planning process and Incident Action Plans (IAPs) are central to managing incidents. The incident action planning process helps synchronize operations and ensure that they support incident objectives.

- An excerpt of the incident action planning process is located in the EOC Toolkit at https://www.fema.gov/emergency-managers/nims/components#eoc

- https://training.fema.gov/emiweb/is/icsresource/assets/incident%20action%20planning%20process.pdf

Lifelines

- FEMA developed the community lifelines construct to increase effectiveness in disaster operations and better position the agency to respond to catastrophic incidents.

- https://www.fema.gov/lifelines

National Incident Management System (NIMS)

- On the NIMS website, users can find links to NIMS documents, guidelines and operational tools, as well as training information, implementation guidance, updates and contact information for the FEMA Regional NIMS Coordinators.

- https://www.fema.gov/emergency-managers/nims/components

National Qualification System (NQS)

- The NIMS Guideline for the NQS describes the components of a qualification and certification system, defines a process for certifying the qualifications of incident personnel, describes how to

[11] This resource contains references to non-federal resources and materials. Such references do not constitute an endorsement by the U.S. government, or any of its employees, of the information or content which a non-federal resource or material provides.

establish and implement a peer review process and introduces the process of credentialing personnel.

- NQS also provides Job Titles/Position Qualifications and Position Task Books (PTBs) for a range of incident management, incident support and emergency management positions.
- https://www.fema.gov/national-qualification-system

NIMS Training Program

- The NIMS Training Program specifies NIC and stakeholder responsibilities and activities for developing, maintaining and sustaining NIMS training.
- https://www.fema.gov/nims-training

NQS EOC Skillsets and EOC Skillsets User Guide

- EOC Skillsets promote a national vocabulary for EOC personnel qualifications and let EOC leaders build position qualifications according to their organization's needs and resources.
- https://www.fema.gov/emergency-managers/nims/components#eoc

OneResponder

- OneResponder, the application supporting NQS, is a web-based expert qualifications system that provides a common language and approach to qualify and certify emergency personnel.
- Personnel Qualifications - National Resource Hub - Preparedness Toolkit (fema.gov)

Threat and Hazard Identification and Risk Assessment (THIRA)

- The THIRA process helps communities understand their risks and determine the capabilities they need to address those risks.
- https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment

Vulnerability Assessment

- The vulnerability assessment is an in-depth analysis of a building's functions, systems and site characteristics to identify the building's weaknesses and lack of redundancy, and to determine mitigations or corrective actions to reduce vulnerabilities.
- https://www.fema.gov/pdf/plan/prevent/rms/155/e155_unit_iv.pdf
- https://training.fema.gov/is/courseoverview.aspx?code=IS-395

Annex

1. Emergency Operation Center (EOC) Self-Assessment Tool

This Annex to the National Incident Management System (NIMS) EOC How-to Quick Reference Guide is a self-assessment tool to help state and local EOC leaders identify operational gaps and areas requiring improvement in the EOC. The self-assessment is a comprehensive tool, though not all-inclusive, for use in two scenarios:

- When planning and setting up a primary EOC or alternate EOC; and
- When reviewing and refreshing an existing EOC, whether primary or alternate.

This tool consists of a series of detailed questions and considerations related to EOC assessment, mitigation, action steps and implementation in six primary areas: Facility Features, Survivability, Security, Sustainability, Interoperability and Flexibility. The questions warrant different responses depending on the EOC's type (state or local) or nature (primary or alternate). Not all items will apply to all EOCs.

2. Tips for Using This Tool

Ideally, EOC leaders will use this self-assessment tool to create a comprehensive plan and checklist, or punch list, of ways to improve their primary or alternate EOC—and will then use their checklist to plan, implement, track and report on improvements. Checklist items can be administrative tasks or operational readiness items. The plan/checklist can provide a baseline profile of the EOC's unique capacity, capability and readiness. It can also inform the EOC's overall planning, coordination, resource management and training/exercise goals.

A few tips can help as you use this tool:

- **Physical space.** When assessing the physical space of an EOC or alternate EOC:
  - Include the area in square feet;
  - Consider the number of staff per shift and requested reasonable accommodations; and
  - Assess ability to accommodate surge operations.
- **Telephone communications.** When assessing communications capabilities, provide sufficient detail to fully assess the adequacy of each capability. With telephones, for example, consider:
  - Number of devices available;

  - Number of lines (phone jacks) in each room; and
  - Capabilities of the phone switch (for example, can the switch support additional phone drops, if required, for surge operations?).

- **Computers.** When assessing computers, consider:
  - Access to network connectivity; and
  - Network's ability to handle increased traffic resulting from increased emergency operations activity.

- **Radio devices.** When assessing radio capabilities:
  - Provide sufficient descriptive information about devices (for example, portable transceiver, radio console);
  - List the number of devices on hand;
  - Determine the quantity necessary to support normal and surge operations; and
  - Consider access to batteries, chargers and spares for portable devices.

- **Other issues.** Be sure to address any concerns or issues not included in the self-assessment questions using the blank page at the end of this document.

- **Timeline.** Many self-assessment questions imply the notion of a timeline for completion (such as when the response is "no" or "not yet"). The Federal Emergency Management Agency (FEMA) has not set deadlines for completing these items but encourages EOC leaders to develop a checklist—with or without associated deadlines—to help identify, categorize, prioritize and track open items.

3. More Information

For more information about how to establish, operate and continuously improve an EOC, see the References and Resources section of the main guide, above.

If you have questions about the content of this EOC Self-Assessment Tool, send an email to FEMA-NIMS@fema.dhs.gov.

4. Facility Features

This category examines the physical features of primary and alternate EOC facilities, including the site, structure, accessibility and capacity. EOC spaces to consider include the Operations Room (Ops Room), conference rooms, communications center, secure communications room and multiuse space. Multiuse space is typically an administrative or conference area that non-EOC staff use for daily functions but then vacate, moving to another location, if EOC staff need it for emergency operations during major disaster or surge situations.

1. Does the primary EOC/alternate EOC already exist?
2. Is the primary EOC/alternate EOC in an urban, suburban or rural area?
3. Is the primary EOC/alternate EOC near a government center, such as a city hall, county courthouse or state capitol?
4. Do government executives/key officials have rapid access to the primary EOC/alternate EOC?
5. Are additional government personnel readily available to augment the primary EOC/alternate EOC should the emergency escalate beyond the on-duty team's capacity?
6. Is the primary EOC/alternate EOC centrally located, allowing rapid response to all parts of the jurisdiction?
7. Is the primary EOC/alternate EOC in a low-congestion area, without transportation chokepoints such as inadequate thoroughfares, bridges, etc.?
8. Does the primary EOC/alternate EOC location minimize the risk of damage from collapsing buildings?
9. Does the primary EOC/alternate EOC facility have structural integrity?
10. Is the primary EOC/alternate EOC in an area that allows experts to secure it quickly, if necessary?
11. Is the primary EOC/alternate EOC in a known high-risk area—for example, in a flood or earthquake zone or near a nuclear power plant or Hazardous Materials (HAZMAT) site? If yes, explain. Are plans in place to mitigate risk?
12. Does the primary EOC/alternate EOC have easy access to an adequate road network?
13. Is the primary EOC/alternate EOC within a building (basement, ground floor, upper floor) or is it below grade in a shelter?
14. Is the building/shelter housing the primary EOC/alternate EOC close to or set back from a tree line?
15. Is the structure for the primary EOC/alternate EOC ADA complaint?
16. Does the primary EOC/alternate EOC have adequate parking? Are the parking spaces above or below ground? In a parking lot or a garage? Are there ADA compliant parking spaces?

17. Does the primary EOC/alternate EOC have space to accommodate a helicopter landing pad? Is the surrounding area sufficiently clear of obstructions to allow a helicopter to approach and land?
18. Is the primary EOC/alternate EOC in a government-owned facility or a leased facility?
19. Does the primary EOC/alternate EOC occupy an independent building/shelter, or does it use space in another organization's facility—for example, is it within a state or local police headquarters, Emergency Medical Services (EMS) facility, National Guard armory or commercial building?
20. Is the primary EOC/alternate EOC dedicated to EOC operations or is it multi-use?
21. Does the primary EOC/alternate EOC consist of one large room or a complex of rooms?
22. Does the primary EOC/alternate EOC have sufficient space for an Ops Room or area (to perform emergency response and management functions), a conference/media area (for meetings and press briefings), a communications center (for centralized fax transmission, radio transmission and videoconferencing) and a secure communications room (for secure voice, fax and video)?
23. Does the primary EOC/alternate EOC have a dedicated Ops Room? If so, is it large enough to support the EOC staff as well as liaison staff from partner agencies and organizations?
24. Does the primary EOC/alternate EOC have a dedicated conference/media room? If so, is it large enough to support meetings and media briefings? Is it physically separated from the operations area so that media briefings do not interfere with ongoing operations?
25. Does the primary EOC/alternate EOC have a dedicated communications center? If so, is the space adequate to support EOC communications requirements?
26. Does the primary EOC/alternate EOC have a secure communications room? If so, is the space adequate to support cleared EOC staff and secure communications requirements?
27. Does the primary EOC/alternate EOC have designated multiuse space? If so, is the space large enough to support expanded operations? Is the space readily available?
28. Can the primary EOC/alternate EOC support supplemental staff from other federal or state agencies in a major disaster or surge situation? If not, is the space reconfigurable, or are there plans in place to provide the necessary additional space?
29. Have experts conducted an electrical audit of the facility to assess capability, fitness and adequacy to support the electrical demands of a primary EOC/alternate EOC operating 24/7?

5. Survivability

This category relates to the EOC's ability to sustain the effects of a realized risk and to continue operating from the primary EOC or a fully capable alternate location—that is, an alternate EOC that can activate if the primary location suffers severe damage or becomes inaccessible.

1. Have leaders identified an alternate EOC location to ensure Continuity of Operations (COOP)?
2. Is the primary EOC/alternate EOC in a known high-risk area—for example, in a flood or earthquake zone or near a nuclear power plant or HAZMAT site?
3. Can the primary EOC/alternate EOC survive the effects of relevant risks, such as natural and human-caused hazards?
4. Does the primary EOC/alternate EOC have special structural features or capabilities that improve its survivability?
5. Does the primary EOC/alternate EOC have a collective protection system for chemical, biological, radiological and nuclear (CBRN) agents?
6. Does the primary EOC/alternate EOC have protection from blast effects?
7. Is the primary EOC/alternate EOC above the ground floor, on the ground floor or below grade?

6. Security

This category relates to guarding against potential risks and protecting operations from the unauthorized disclosure of sensitive information—that is, ensuring sufficient security and structural integrity to protect the facility, its occupants, its communications equipment and its systems from relevant threats and hazards.

6.1. Facility

1. Is the primary EOC/alternate EOC in an urban, suburban or rural area?
2. Are physical security measures (barriers, security cameras, etc.) already in use in the primary EOC/alternate EOC? Are these existing security features adequate? If not, what additional security features, such as access controls, barriers, secure areas and surveillance devices, are required?
3. What systems are in place to control access to, and within, the primary EOC/alternate EOC? Is a badge or card-swipe system in use? Are the systems adequate to control access to the facility and within the facility?
4. Does appropriate staff have 24-hour access to the primary EOC/alternate EOC?
5. Are there any access control systems (card access systems, elevators, lock-out stairwells) that, if nonoperational, could prevent access to the primary/alternate EOC facility? If yes, what alternate plans are in place to ensure access?
6. What, if any, plans are in place to increase security capabilities at the primary EOC/alternate EOC as threat levels rise? Examples include adding barriers, increasing surveillance and adding guards.
7. Do authorized staff have access to secure spaces where they can discuss classified or sensitive information in isolation from unauthorized/uncleared individuals at the primary EOC/alternate EOC?
8. Does the primary EOC/alternate EOC have a secure communications room? Does it meet FEMA security requirements? Is the square footage of the room adequate?
9. What systems are in place to control access to the secure communications room at the primary EOC/alternate EOC? Are existing controls adequate?

6.2. Communications/Networks

1. Do local area networks (LAN) supporting emergency operations at the primary EOC/alternate EOC have adequate protection against cyberattacks (unauthorized access, denial of service, malicious code, etc.)? If not, what capabilities are necessary?

2. Do statewide wide area networks (WAN) supporting emergency operations have adequate protection against cyberattacks (unauthorized access, denial of service, malicious code, etc.)? If not, what capabilities are necessary?
3. Does the primary EOC/alternate EOC have a secure voice capability? If so, is it adequate to support emergency operations?
4. Do nonsecure telephones at the primary EOC/alternate EOC have a privacy feature?
5. Does the primary EOC/alternate EOC have a secure fax capability? If so, is it adequate to support emergency operations?
6. Are radio communications at the primary EOC/alternate EOC protected (encrypted)? Do these radios have privacy features?
7. Does any of the telecommunications/internet capabilities rely on external equipment?

6.3. Personnel

1. Is security clearance required for personnel at the primary EOC/alternate EOC?
2. If so, do cleared personnel receive training in the following?
3. Using secure communications equipment
4. Controlling and protecting classified material
5. Managing and controlling communications security
6. Do individuals with security clearance have the appropriate identification, such as a unique mark on their identification badge?

7. Sustainability

This category relates to supporting operations for extended durations. The primary EOC/alternate EOC should be able to sustain operations 24/7 during all emergencies without interruption. It should, to the extent possible, be in an area that is not at considerable risk for known hazards. For example, planners should avoid flood zones, earthquake zones and areas near nuclear power plants and HAZMAT sites.

7.1. Facility

Can the primary EOC/alternate EOC support 24/7 operations for an extended period? Are the operational and administrative supplies—food, water, fuel for backup generators, paper products, office supplies, etc.—adequate to sustain operations?

1. Does the primary EOC/alternate EOC have backup power (typically generator power)?
2. Does the primary EOC/alternate EOC have an Uninterruptable Power Supply (UPS) unit? (UPS units typically use batteries to provide power for a limited duration—perhaps 10 or 20 minutes, depending on the load.) If yes, what systems/functions does the UPS support? Is the duration of the UPS adequate to support these systems/functions until the backup power comes online?
3. Do heating, ventilation and air conditioning (HVAC) systems at the primary EOC/alternate EOC have central, building-wide management or local management?
4. Are the HVAC systems at the primary EOC/alternate EOC available and controllable 24/7?
5. Does the primary EOC/alternate EOC have access to support areas, such as file rooms, server sites, etc.?
6. What, if any, special constraints or special access needs could interfere with sustained operations at the primary EOC/alternate EOC?
7. Does the alternate EOC have the same capabilities as the primary location? If not, what are the differences?

7.2. Communications/Networks

Is the number of telephones, both secure and nonsecure, adequate for the primary EOC/alternate EOC to conduct emergency response and management operations?

1. Are telephones connected via Voice over Internet Protocol (VoIP) technology at the primary EOC/alternate EOC?
2. Are telephones at the primary EOC/alternate EOC hardwired, with a direct connection to a local commercial carrier (and a dial tone from the local switch) rather than connected via VoIP technology? (The advantage is that if the EOC loses power, hardwired phones should continue to function.)

3. Does the primary EOC/alternate EOC have dedicated machines for transmitting and receiving faxes?
4. Is the number of fax machines, both secure and nonsecure, adequate to conduct emergency response operations at the primary EOC/alternate EOC?
5. Does the primary EOC/alternate EOC have secure fax capabilities?
6. Does the primary EOC/alternate EOC have enough printers to conduct ongoing emergency response operations?

8. Interoperability

This category involves sharing common operating principles and exchanging routine and time-sensitive information among local jurisdictions, state-level EOCs and FEMA's network of operations centers. An EOC should be able to communicate with key state agencies, local government EOCs, emergency response teams at or near an incident site, neighboring state EOCs and federal authorities, including the FEMA Regional Operations Center (ROC) and the FEMA Operations Center.

8.1. Communications

8.1.1. REQUIREMENTS

1. Does the primary EOC/alternate EOC have a requirement to monitor the communications of key emergency services—police, fire, EMS, HAZMAT and public works—or of other services? If so, does the capability exist and is it adequate?
2. Does the primary EOC/alternate EOC have a requirement to establish an emergency communications network that includes the key emergency services and local EOCs/jurisdictions? If so, does the capability exist and is it adequate?
3. If a requirement exists, can the primary EOC/alternate EOC communicate with the following entities?
    - Local EOCs throughout the state;
    - FEMA ROC and FEMA regional staff;
    - FEMA Disaster Field Office;
    - Primary EOC/alternate EOC locations in other states;
    - Operations centers of state-level emergency services organizations;
    - Incident Commanders (IC) or Incident Command Post (ICP); and
    - Operations centers of the regional and local airport, highway, port and waterway authorities; hospitals and ambulance service providers; nuclear power plants; dams; private sector utilities (power, telephone, sewer and water) and chemical companies.
4. Are the communications means at the primary EOC/alternate EOC adequate to meet communications requirements? Consider radios, telephones, cell phones, available frequency spectrum and other issues.

8.1.2. RADIOS

1. Do agencies provide radios, or are radios part of the primary/alternate EOC project?

2. Is the installation at the primary EOC/alternate EOC temporary (requiring handheld radios) or permanent (requiring a radio base station)?
3. If agencies provide radios, do they require power and antenna hookups for extended operations?
4. Do radios reside in the Ops Room or a separate communications room at the primary EOC/alternate EOC?
5. Could different radio systems create interference with each other?
6. Are chargers necessary for radios, cell phones, pagers, etc.?

8.2. Procedures

1. Do state and local government EOCs, both primary and alternate, have common operations, reporting and communications procedures to follow during an all-hazards event response?
2. If the primary EOC/alternate EOC has a requirement to exchange information with local EOCs/jurisdictions and key emergency services—police, fire, EMS, HAZMAT and public works—are procedures and checklists in place to facilitate the process?
3. Does the primary EOC/alternate EOC have a process for assembling and disseminating scheduled reports, if required?

8.3. Training

1. Do state and local government primary/alternate EOCs conduct routine, recurring or periodic joint communications training events to exercise the communications capabilities necessary for responding to an all-hazards event?
2. If so, do leaders record the results of joint communications training in a “lessons learned” document and use them to improve communications operations? Do they also use the results to identify communications deficiencies and develop solutions that correct the deficiencies and improve communications capabilities?
3. Do state and local government primary/alternate EOCs conduct routine, recurring or periodic joint training exercises to practice, test and refine their common operations, reporting and communications procedures?
4. If so, do leaders record the results of joint training in a “lessons learned” document and use them to improve common procedures?
5. Do EOC leaders use actual experiences to validate existing common procedures and create new ones?

9. Flexibility

This category has to do with scaling operations and adapting the operational pace to the all-hazards event. For example, the primary EOC/alternate EOC should have sufficient space, equipment, furniture, administrative supplies, etc., to meet mission requirements.

9.1. Facility

9.1.1. PRIMARY EOC

1. Is the primary EOC facility dedicated to EOC operations? If not, does the EOC occupy space in another organization's facility—for example, is it within a state or local police headquarters, EMS facility, National Guard armory or commercial building?
2. Whether the facilities are dedicated or shared, is the square footage available to the EOC adequate to conduct emergency response operations?
3. Is the EOC operational only during emergency response and management operations? Or is the EOC operational 24/7, with staff and capabilities present and active whether or not an emergency response is underway?
4. Are activation, layout and setup procedures in place for the EOC?
5. Are the plans and procedures in place to tailor the EOC's activation and operations to the scale of emergency response activities? (For example, a small-scale event might require fewer staff/capabilities and limited emergency response operations; a large-scale event might require all staff, full capabilities and extensive emergency response operations.)
6. Have leaders identified the conditions that would cause the EOC to move to the alternate location? Are relocation procedures in place?
7. Do leaders hold EOC activation and relocation exercises periodically? If so, are member agencies' participation levels sufficient to ensure efficient and timely activation during actual events? Do participants include key EOC personnel?
8. Does the EOC have a dedicated conference/media room? If so, is the square footage adequate?
9. Does the EOC have access to multiuse space? If so, is the square footage adequate?

9.1.2. ALTERNATE EOC

1. Does an alternate EOC already exist to ensure COOP for emergency response operations?
2. Is the alternate EOC facility dedicated to EOC operations? If not, does the EOC occupy space in another organization's facility—for example, a state or local police headquarters, EMS facility, National Guard armory or commercial building?
3. Whether the facilities are dedicated or shared, is the square footage available to the alternate EOC adequate to conduct emergency response operations?

4. Are activation, layout and setup procedures in place for the alternate EOC?
5. Are the plans and procedures in place to tailor the alternate EOC's activation and operations to the scale of emergency response activities?
6. Have leaders identified the conditions that would cause the alternate EOC to activate in place of the primary EOC?
7. Does the alternate EOC have the same capabilities as the primary EOC? If not, what are the differences?
8. Do leaders hold alternate EOC activation exercises periodically? If so, are member agencies' participation levels sufficient to ensure efficient and timely activation during actual events? Do participants include key EOC personnel?
9. Does the alternate EOC have a dedicated conference/media room? If so, is the square footage adequate?
10. Does the alternate EOC have access to multiuse space? If so, is the square footage adequate?

9.2. Communications/Networks

1. Is the number of computers in the primary EOC/alternate EOC and any multiuse space adequate to support emergency response operations?
2. Is the number of servers in the primary EOC/alternate EOC adequate to support emergency response operations?
3. Is the number of telephones, both secure and nonsecure, in the primary EOC/alternate EOC and any multiuse space adequate to support emergency response operations?
4. Are telephones in the primary EOC/alternate EOC and any multiuse spaces hardwired, with a direct connection to a central local office rather than connected via VoIP technology? (The advantage is that if the EOC loses power, hardwired phones should continue to function.)
5. Do any telephones have the following capabilities?
    - Audio recording
    - Caller ID
    - Voice conferencing
6. Is the number of printers in the primary EOC/alternate EOC and any multiuse space adequate to support emergency response operations?
7. Is the number of fax machines in the primary EOC/alternate EOC and any multiuse space adequate to support emergency response operations?

8. Do the primary EOC/alternate EOC and any multiuse space have video display capabilities? If so, do they also have the capability to play the audio associated with the video?
9. Do the primary EOC/alternate EOC and any multiuse space have videoconferencing capabilities?
10. Do the primary EOC/alternate EOC and any multiuse space have the capability to receive public/intercom announcements?
11. Can telecommunications capabilities in the primary EOC/alternate EOC scale to support surging emergency response and management activities?
12. Are appropriate cables and adapters available to connect different computers to the display system?

10. Other Considerations

Geographic data and analysis capability

- Does the primary EOC/alternate EOC have access to geospatial information for the jurisdiction—maps, imagery and GIS?

Hazard prediction and monitoring capability

- Does the primary EOC/alternate EOC have hazard prediction capabilities (models) that can plot and predict downwind hazards resulting from chemicals or radioactive fallout?
- Does the primary EOC/alternate EOC have hazard protection capabilities (models) and monitors for natural hazards—such as flood gauges, tsunami warning systems or seismic monitoring systems?

Crisis information management system

- Does the primary EOC/alternate EOC have a crisis information management system that integrates relevant information so users can access it quickly and efficiently?

Personnel qualification and certification system

- Does the primary EOC/alternate EOC have a system to track qualified and certified personnel within the jurisdiction?

11. Additional Comments and Other Key Information

(Use this section for your organization's specific information, notes and next steps)