Prerequisite

Before you can take the FEMA exams, you will need to register with the FEMA System Identification System to get a SID.

Links

- National Disaster & Emergency Management University
- SID registration
- Course page
- Interactive course

Overview

IS-700 (also labeled IS-700.B) is an introduction to the NIMS, or National Incident Management System.

To receive credit for the course, you must get a 75% or higher on the final exam. The exam is accessible from the course page.

Lesson 1: Fundamentals and Concepts of NIMS

NIMS, the National Incident Management System, is a comprehensive and standardized framework designed to be usable across all potential incidents, regardless of cause, size, location, or complexity. It is designed to ensure that all levels of government, NGOs, and private sector organizations can work together seamlessly to prevent, protect against, mitigate, respond to, and recover from the incidents. It can also be used for planned events, such as sports.

While NIMS provides a framework for many things, it is important to remember that it provides organization and procedures and that those involved in the incident have to handle the final logistics for many things. For example, NIMS provides procedures for resource management coordination across different groups and principles for communications/information management, but NIMS itself does not provide resources or a specific communications plan.

The three guiding principles behind NIMS are:

1. Flexibility
    1. NIMS should be usable for anything from a routine, local incident to one requiring interstate mutual aid or even federal assistance
    2. It should be applicable to incidents that vary wildly in terms of hazard, geography, demographics, climate, culture, and organizational authorities
    3. It should be usable for planned events (e.g., concerts or sports), forecasted events (e.g., hurricanes), and events with little or no notice (e.g., a tornado)
2. Standardization
    1. Defines **standard organizational structures** that improve integration and connectivity among involved organizations
    2. Defines **standard practices** that allow incident personnel and organizations to work together effectively
    3. Includes **common terminology** to enable effective communication
3. Unity of Effort

    1. Unity of Effort simply means coordinating activities among various groups to achieve common objectives
    2. Organizations with jurisdictional authority or functional responsibilities should support each other while also allowing other participating agencies to maintain their own authorities and accountabilities

The major components to NIMS are Resource Management, Command and Coordination, and Communications and Information Management.

Resource Management describes mechanisms to manage resources (personnel, equipment, supplies, teams, facilities), both before and during incidents, in order to allow organizations to more effectively share necessary resources.

Command and Coordination is the leadership roles, processes, and organizational structures for incident management.

Communications and Information Management describes systems and methods to ensure that personnel and decision makers have a means of communication and necessary information to allow them to make and communicate decisions.

Lesson 2: NIMS Resource Management

Resource management involves collaboration and coordination between jurisdictions and organizations to manage various types of resources. This is necessary since most jurisdictions and organizations are unable to own and maintain all resources that may be needed to address any potential threat or hazard, so they work with others to leverage resources.

There are four key activities to for resource management:

1. Identifying and typing resources
    1. Resource typing defines and categorizes resources by capability
    2. Establishes common definitions for the capabilities of resources
    3. Typing definitions include:
        1. **Capability**: the resource's capability to perform its function in one or more of the five mission areas (Prevention, Protection, Mitigation, Response, Recovery)
        2. **Category**: the function for which a resource would be most useful (e.g., firefighting, law enforcement, health, medical, communications)
        3. **Kind**: a broad characterization (e.g., personnel, equipment, team, facility)
        4. **Type**: level of capability to perform its function based on size, power, capacity, experience, qualifications (Type 1 has the greatest capability, Type 4 the smallest)
    4. See the Resource Typing Library Tool for examples of resources and their types
2. Qualifying, certifying, and credentialing personnel
    1. The AHJ, or Authority Having Jurisdiction, is responsible for qualification, certification, and credentialing within an organization/jurisdiction
    2. **Qualifying**: personnel can meet the minimum established standards (training, experience, physical and medical fitness) to fill specific positions
    3. **Certification**: recognition from an AHJ or a third party that an individual has completed qualification for a position (e.g., state board for a medical professional)
    4. **Credentialing**: the documentation that identifies personnel and verifies their qualifications (e.g., an ID card or badge)
3. Planning for resources

    1. Jurisdictions and organizations work together *before* incidents to develop plans identifying, managing, estimating, allocating, ordering, deploying, and demobilizing resources
    2. This includes identifying resource requirements for anticipated threats and vulnerabilities
    3. RM planning should consider resources for all mission areas: Prevention, Protection, Mitigation, Response, Recovery
    4. Planners should consider stockpiling resources, establishing mutual aid agreements, determining how and where to assign resources performing non-essential tasks, and developing contracts with vendors for resource acquisition
4. Acquiring, storing, and inventorying resources
    1. Organizations acquire, store, and inventory resources as a normal day-to-day activity
    2. Effective resource management requires a current and accurate inventory of resources, whether it's as simple as a spreadsheet on a sheet of paper or a fancy computer inventory system
    3. As far as NIMS is concerned, resource inventorying refers to preparedness activities performed outside of incident response
        1. Resource *tracking* occurs during an incident

During an Incident, Resource Management involves the following six tasks:

1. Identify Requirements
    1. Identify the type and quantity of resources needed, location where resources should be sent, and who will receive and use the resources
    2. The type and quantity of resources, as well as their availability, changes as an incident progresses so incident management personnel must continually identify, validate, and refine their resource needs
2. Order and Acquire
    1. This one is pretty self-explanatory
    2. Incidents require resources, and they must ordered
    3. If resources are needed that are not available locally (within the jurisdiction/organization), they can be ordered by executing contracts, implementing mutual aid agreements, or requesting assistance from another level of government
        1. The external jurisdiction/organization must consent to the request
    4. NIMS resource typing helps ensure that a resource meets the specific needs
3. Mobilize
    1. Resources begin mobilizing ("deploying") when notified through established channels
        1. Fixed facility resources are "activated" rather than "deployed"
    2. Personnel being deployed receive the following information:
        1. Date, time, and place of departure
        2. Mode of transportation to the incident
        3. Estimated date/time of arrival
        4. Reporting location and assigned supervisor
        5. Anticipated incident assignment
        6. Anticipated duration of deployment
        7. Resource order number
        8. Incident number
        9. Applicable cost and funding codes
    3. Upon arrival, resources check in according to the receiving organization's check in process
    4. Responders sometimes arrive without being requested
        1. This interferes with incident management:
            1. Creates additional supervisory, logistical, and safety needs

        2. Depletes available resources
        3. Complicates resource tracking and accountability
        4. Interferes with access to the site by formally requested resources
    2. Responders should wait for official deployment notification and not self-deploy

4. Track and Report
    1. Resources are tracked from mobilization through demobilization using established resource tracking procedures that:
        1. Track the location of resources
        2. Help staff prepare to receive and use resources
        3. Protect the safety and security of resources
        4. Enable resource coordination and movement

5. Demobilize
    1. The goal of demobilization is the orderly, safe, and efficient return of a resource to its original location and status
    2. Managers begin planning and preparation for the demobilization process at the same time they begin mobilizing resources
    3. As resources are no longer needed, they should be reassigned or demobilized
    4. Prior to demobilization, incident planning and logistics personnel plan for rehab, replenishment, disposal, and/or return/restoration to operational condition for the resources

6. Reimburse and Restock
    1. Reimbursement provides for payment of expenses incurred by resource providers
    2. Reimbursement procedures are often specified in mutual aid and assistant agreements

Mutual aid agreements establish the legal basis for two or more entities to share resources. There are many mutual aid agreements and compacts within the US, including between two or more neighboring communities, among all jurisdictions within a state, between states/territories/tribal governments, between federal agencies, internationally, between government and NGOs/private sector, and among NGOs/private sector entities. When receiving a request for mutual aid, the supporting jurisdiction determines if it would still be able to meet its own requirements during the temporary loss of resources.

EMAC (Emergency Management Assistance Compact) is a mutual aid compact ratified by Congress that defines a non-federal state-to-state system for sharing resources across state lines during an emergency or disaster. It has been signed by all 50 states, DC, Puerto Rico, Guam, and the US Virgin Islands.

Lesson 3: NIMS Management Characteristics

The NIMS Management Characteristics are available in the IS-100 document, Unit 2.

Lesson 4: Incident Command System (ICS)

Most of the information regarding the ICS is available in the IS-100 document.

Common Types of ICS Facilities

- Incident Command Post (ICP)
    - Location of the tactical-level, on-scene incident management (Incident Commander or Unified Command and Staff)
- Staging Areas

    - Temporary position
    - Accounts for personnel, supplies, and equipment awaiting assignment
- Incident Base
    - Location at which personnel conduct primary support activities
    - May be co-located with the ICP
- Camps
    - Satellites to an Incident Base
    - Established where they can best support incident operations by providing food, sleeping areas, sanitation, and minor maintenance and servicing of equipment

Incident Management Teams and Incident Management Assistant Teams

IMTs are a rostered group of ICS-qualified personnel composed of an Incident Commander, other incident leadership, and personnel qualified for other key ICS positions. They are established at local, regional, state, tribal, and national levels with formal notification, deployment, and operational procedures in place. IMTs are typed based on team member qualifications and are assigned to manage incidents or to accomplish supporting incident-related tasks or functions. When assigned to an incident, an IMT is typically delegated the authority to act on behalf of the affected jurisdiction/organization.

Some IMTs are referred to as IMATs as a clarification that they **support** the on-scene personnel and/or the affected jurisdiction/organization.

Area Command

An Area Command organization oversees the management of multiple incidents or a single very complex incident and is only activated for an incredibly complex incident or to alleviate span-of-control issues. It is useful for situations with several ICPs that are requesting similar, scarce resources. They may be organized as a Unified Area Command, following the same principles as a Unified Command.

Lesson 5: Emergency Operations Centers (EOC)

An EOC is an off-site location where staff from multiple agencies join to address imminent threats and hazards and provide coordinated support to incident command, on-scene personnel, and/or other EOCs. Their purpose, authority, and composition vary wildly, but they generally perform the following functions:

- Collect, analyze, and share information
- Support resource needs and requests (including allocation and tracking)
- Coordinate plans and determine both current and future needs
- Possibly provide coordination and policy direction

An EOC can be a fixed location, a temporary facility, or virtual.

EOC teams are, like ICS, organized modularly. NIMS identifies three common organizations for EOC teams:

1. ICS or ICS-like structure
    1. This structure will be similar or identical to the ICS structure, with the EOC's director at the top (like an Incident Commander or Unified Command)
    2. Operations, Planning, Logistics, and Finance/Administration groups may exist under the director
2. Incident Support Model structure
    1. The ISM structure is often used by groups that choose to focus their EOC on information, planning, and resource support

    2. Groups under the EOC director may include Situational Awareness, Planning Support, Resources Support, and Center Support.
3. Departmental structure
    1. The departmental structure uses the day-to-day structure of the department/agency. In this case, the normal segmentation of the agency (e.g., public works, fire, law enforcement) operate as their own branches underneath the EOC director.
    2. This structure has minimal preparation and startup time.

Reasons that an EOC may be activated include:

- Multiple jurisdictions or agencies are involved in an incident
- The IC or Unified Command indicates an incident could expand rapidly, involving cascading effects or requiring additional resources
- A similar incident in the past led to an EOC activation
- The EOD director (or an appointed/elected official) directs EOC activation
- An incident is imminent such as a predicted hurricane, flooding, hazardous weather, or elevated threat levels
- Threshold events described in an emergency operations plan occur
- Significant impacts to the population are anticipated

EOCs frequently have multiple activation levels to allow for the response to be appropriately scaled, appropriate coordination for the incident, and delivery of only the needed resources.

	Activation Level	Description
3	Normal Operations/Steady State	- Activities that are normal for the EOC when no incident or specific risk or hazard has been identified - Routine watch and warning activities if the EOC normally houses this function
2	Enhanced Steady-State/Partial Activation	Certain EOC team members/organizations are activated to monitor a credible threat, risk, or hazard and/or to support the response to a new and potentially evolving incident
1	Full Activation	EOC team is activated, including personnel from all assisting agencies, to support the response to a major incident or credible threat

Lesson 6: Other NIMS Structures and Interconnectivity (MAC, JIS)

Multiagency Coordination Groups (MAC Groups)

MAC groups, sometimes referred to as policy groups, are part of the off-site incident management structure of NIMS. Members are typically agency administrators, executives, or their designees from involved agencies/organizations impacted by and with resources committed to the incident.

During an incident, a MAC group will act as a policy-level body making cooperative decisions between agencies and supporting resource prioritization and allocation. It does not, however, perform any incident command functions, nor does it replace EOCs.

Joint Information System (JIS)

The JIS combines public affairs and incident information into a single organization, providing information to the public and stakeholders during incident operations. The JIS' activities include:

- Develop and deliver interagency messages
- Develop, recommend, and execute public information plans/strategies
- Advise on public affairs issues that could affect the incident management effort
- Address and manage rumors and inaccurate information that could undermine public confidence

The JIC (Joint Information Center) is a central location that houses JIS operations. An incident should typically only have a single JIC, but NIMS allows for multiple if deemed necessary.

The PIO (Public Information Officer) is a key member of ICS and EOC organizations (they may use a different title in an EOC). Among their duties are:

- Advise the IC, Unified Command, or EOC director on public information matters
- Gather, verify, coordinate, and disseminate information in an accurate, accessible, and timely manner
    - Gather complete information for the public and other stakeholders
    - Verifying information to ensure accuracy
    - Coordinating information with other public information personnel who are part of the JIS to ensure consistency
    - Disseminating consistent, coordinated, accurate, accessible, timely, and complete information to the public and stakeholders
- Handle inquiries from the media, the public, and elected officials
- Provide emergency public information and warnings
- Conduct rumor monitoring and response

Public information communication plans should be included in training and exercises, as public information may include lifesaving measures and evacuation routes. Plans should include draft news releases, media lists, and contact information for elected/appointed officials, community leaders, private sector organizations, and public service organizations.

Most incidents are resolved with capabilities and resources from the local jurisdiction, expanding to include neighboring jurisdictions or State, tribal, territorial, and interstate sources if the incident is large enough. The federal government only gets involved, typically in a supporting role, in incident response when:

- State governors or tribal leaders request federal assistance and the request is approved
- Federal interests are involved (e.g., an incident occurs on federal property or the federal government has primary jurisdiction)
- A statute or regulation authorizes or requires federal involvement

Lesson 7: Communications and Information Management

Effective incident management requires communications and information systems that provide timely, accurate, and relevant information to everyone involved. There are four key communications and information systems principles that support incident managers to maintain proper flow of information during an incident:

1. Interoperability
    1. The capacity for emergency management and response personnel to interact and work well together
        1. Within and across jurisdictions and organizations
        2. Over voice, data, and video systems

        3. In real time

2. Reliability, scalability, and portability
    1. Reliable: familiar to users, adaptable to new technology, and dependable in any situation
    2. Portable: can be transported, deployed, and integrated easily to enable support of incidents across jurisdictions
    3. Scalable: can expand to support any incident, small or large, and support a rapid increase in the number of users
3. Resilience and redundancy
    1. Resiliency: withstand and continue to perform after damage to or loss of infrastructure
    2. Redundancy: duplicate systems enable continuity through alternate communication methods when primary methods fail
4. Security
    1. Some incident information is sensitive, so communications systems should be able to be secured to the appropriate level to control access to sensitive/restricted information
    2. Communications and information sharing should also comply with data protection and privacy laws

The following are four standard communication types

1. Strategic Communications
    1. High-level directions, including resource priority decisions, roles and responsibilities determinations, and overall incident management courses of action.
2. Tactical Communications
    1. Communications among and between on-scene command and tactical personnel and cooperating agencies and organizations.
3. Support Communications
    1. Coordination of support of strategic and tactical communications (e.g., communications among hospitals concerning resource ordering, dispatching, and tracking; traffic and public works communications).
4. Public Communications
    1. Alerts and warnings, press conferences.

All stakeholders should be involved in communications planning. This planning should determine what systems/platforms are used, who can use the systems, what information is essential, and what the technical requirements are for equipment/systems. These plans should be made into formal agreements and should include things such as the connection of separate networks, data format standards, and cybersecurity agreements.