

---

## Session No. 34

---

**Course Title: Disaster Response Operations and Management**

**Session Title: National Incident Management System (NIMS)**

**Time: 50 minutes**

---

### **Objectives:**

- 34.1 Provide background information about why the National Incident Management System (NIMS) was established.
  - 34.2 Identify the goals of the National Incident Management System (NIMS).
  - 34.3 Define the National Incident Management System (NIMS) and mention the principles under which it operates.
  - 34.4 Discuss the components of the National Incident Management System (NIMS).
  - 34.5 Determine the strengths and weaknesses of the National Incident Management System.
- 

### **Scope:**

This session follows up on the previous two sessions but discusses the nature of the National Incident Management System. The professor first declares why the United States government saw the need for the National Incident Management System, paying close attention to the problematic response on September 11, 2001. The session then reviews the recommendations of two Presidential Directives (HSPD – 5 and HSPD – 8) before defining the National Incident Management System (NIMS). Afterwards, the professor discusses the components, structure and principles under which the National Incident Management System operates. The session is concluded as students work in groups to uncover the strengths and weaknesses of the National Incident Management System.

---

### **Session Requirements:**

1. Instructor Reading:

Bush, George W. 2003. "Homeland Security Presidential Directive/HSPD-5." <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html>

Bush, George W. 2003. "Homeland Security Presidential Directive/HSPD-8." <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>

FEMA. 2004. "Department of Homeland Security Establishes National Incident Management System Integration Center." <http://www.fema.gov/news/newsrelease.fema?id=12385>

FEMA. 2004. "Fact Sheet: National Incident Management System (NIMS)." <http://www.dhs.gov/dhspublic/display?theme=14&content=3697>

FEMA. 2004. "National Incident Management System (NIMS), An Introduction." IS-700. <http://training.fema.gov/EMIWeb/IS/is700.asp>

FEMA. 2004. "The National Incident Management System (NIMS) Integration Center." <http://www.fema.gov/news/newsrelease.fema?id=12385>

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report*. W.W. Norton: New York.

2. Student Readings:

FEMA. 2004. "National Incident Management System (NIMS), An Introduction." IS-700. <http://training.fema.gov/EMIWeb/IS/is700.asp>

and/or

Bush, George W. 2003. "Homeland Security Presidential Directive/HSPD-5." <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html>

Bush, George W. 2003. "Homeland Security Presidential Directive/HSPD-8." <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>

3. Overhead Transparencies/handouts:

Problems Identified in the 9/11 Commission Report  
NIMS Components  
NIMS Strengths and Weaknesses

---

## Remarks:

1. The National Incident Management System is closely related to - but different than - incident command and emergency operations centers. For this reason, the professor may wish to review the findings and the lessons of the prior two sessions.
2. The professor should understand that, at the time of this writing, there was no academic literature on the National Incident Management System. Therefore, it is advisable that a literature search be conducted on the topic before the session is taught.
3. Because the National Incident Management System is currently a work in progress, the Federal government will roll out additional sections, elements or refinements over time. Thus, the professor should survey the FEMA website in order to obtain updated information.
4. Students may need additional assistance identifying the strengths and weaknesses of NIMS. They might not be familiar with the former Federal Response Plan, and they may not appreciate the impact of 9/11 on national emergency management policy.
5. There may not be a large number of individuals who are familiar with or who have expertise in the National Incident Management System. However, the federal government is funding a number of training sessions on NIMS. Possible guest speakers for this session may include those conducting these training activities or those who have participated in the orientation sessions.

---

### **Objective 34.1      Provide background information about why the National Incident Management System (NIMS) was established.**

Present the following as a lecture:

- I. The **National Incident Management System owes its existence** to two sources.
  - First, **NIMS is an offspring of FIRESCOPE and the National Interagency Incident Management System**, which was developed in 1980 by the United States Department of Agriculture Forrest Service to fight fires and deal with other types of disasters (see <http://www.fs.fed.us/fire/operations/niims.shtml>).
  - Second, NIMS was an outgrowth of the **unique, well-publicized, complicated and deadly disaster incidents** that have occurred in recent years.

- A. For instance, the breakup of the **NASA's** space ship, **Columbia**, over Texas in February 2003 presented **unprecedented debris collection challenges** due to the widespread scattering of shuttle fragments. The response to this event **also included organizations** (e.g., NASA) that had heretofore **not been involved** in any type of **disaster response**.
  - B. The **mailing of letters** containing **anthrax spores** to various locations in Florida and Washington, D.C. **illustrated**:
    - 1. the **complexity of biological terrorism**,
    - 2. the **need** to provide detailed **information** to the **public**,
    - 3. and the **importance** of improving **coordination** with **law enforcement** and **public health organizations**.
  - C. But it was really **the terrorist attacks on 9/11** that really **underscored** the **need** for an **improved and broader approach** to the **management of disaster operations**.
  - D. Although the **heroic efforts of first responders** to deal with the terrorist attacks on the **World Trade Center** towers **saved** the **lives** of a number of tenants and visitors in these buildings, it soon **became very evident** that a number of **problems confronted emergency personnel**.
  - E. Under pressure from victims' families, a bi-partisan **committee** was formed to **review failures and mistakes** related to **intelligence gathering**, **counter-terrorism operations**, and **emergency response** to the terrorist attacks. **After** months and even years of **investigation**, the committee released its findings in the **9/11 Commission Report**.
- II. The 9/11 Commission **Report identified** a plethora of **inter-related weaknesses** made evident **in the response**.
- A. **Communications Technology**
    - 1. **"Most Port Authority police commands used ultra-high-frequency radios. Although all the radios were capable of using more than one channel, most PAPD officers used one local channel. The local channels were low-wattage and worked only in the immediate vicinity of that command. The PAPD also had an agency wide channel, but not all commands could access it"** (National Commission on Terrorist Attacks 2004, 281).

2. **“The radios’ signals often did not succeed in penetrating the numerous steel and concrete floors that separated [FDNY] companies attempting to communicate”** (National Commission on Terrorist Attacks 2004, 283).
3. **“As units climbed higher, their ability to communicate with chiefs on tactical 1 became more limited and sporadic, both because of the limited effectiveness of FDNY radios in high-rises and because so many units on tactical 1 were trying to communicate at once”** (National Commission on Terrorist Attacks 2004, 298).
4. **“The means of transmitting information were unreliable”** (National Commission on Terrorist Attacks 2004, 301).

#### B. **Communications Procedures**

1. **“There were no standard operating procedures covering how different [Port Authority] commands should communicate via radio during such an incident”** (National Commission on Terrorist Attacks 2004, 282).
2. **“At 9:05, FDNY chiefs tested the WTC complex’s repeater system. Because the second button had not been activated, the chief on the master handset could not transmit. He was also apparently unable to hear another chief who was attempting to communicate with him from a portable radio”** (National Commission on Terrorist Attacks 2004, 298).

#### C. **Information Management**

1. **“The deputy fire safety director in the lobby, while immediately aware that a major incident had occurred, did not know for approximately ten minutes that a commercial jet had directly hit the building”** (National Commission on Terrorist Attacks 2004, 286).
2. **“At about this time, an announcement over the public-address system in the South Tower stated that the incident had occurred in the other building and advised tenants, generally, that their building was safe and that they should remain on or return to their offices or floors”** (National Commission on Terrorist Attacks 2004, 288).
3. **By 9:30, chiefs in charge of the South Tower still were in need of additional companies. Several factors account for the a lag**

**in response. First, only two units that had been dispatched to the North Tower prior to 9:03 reported immediately to the South Tower. Second, units were not actually sent until approximately five minutes after the FDNY Chief of Department ordered their dispatch”** (National Commission on Terrorist Attacks 2004, 300).

4. **At 9:37, a civilian on the 106<sup>th</sup> floor of the South Tower reported to a 911 operator that a lower floor – the 90-something floor – was collapsing. This information was conveyed inaccurately to the 911 operator to an NYPD dispatcher”** (National Commission on Terrorist Attacks 2004, 304).
5. **“Most of the evacuation instructions did not mention that the South Tower had collapsed”** (National Commission on Terrorist Attacks 2004, 307).

#### **D. Interorganizational Coordination**

1. **“By 8:57, FDNY chiefs had instructed the PAPD and building personnel to evacuate the South Tower as well, because of the magnitude of the damage caused by the first plane’s impact. These critical decisions were not conveyed to 911 operators or to DDNY dispatchers.”** (National Commission on Terrorist Attacks 2004, 287).
2. **“Both FDNY and NYPD protocols called for FDNY personnel to be placed in NYPD helicopters in the event of an attempted rooftop rescue at a high-rise fire. No FDNY personnel were placed in NYPD helicopters on September 11<sup>th</sup>”** (National Commission on Terrorist Attacks 2004, 292).
3. **“Those who had been in the North Tower lobby had no way of knowing that the South Tower had suffered a complete collapse”** (National Commission on Terrorist Attacks 2004, 306).
4. **“The NYPD’s 911 operators and FDNY dispatch were not adequately integrated into the emergency response”** (National Commission on Terrorist Attacks 2004, 318).
5. **“The response operations lacked the kind of integrated communications and unified command contemplated in the directive [an updated directive by Mayor Giuliani regarding the Direction and Control of Emergencies in the City of New York] (National Commission on Terrorist Attacks 2004, 319).**

6. **“There was a lack of comprehensive coordination between FDNY, NYPD, and PAPD personnel climbing above the ground floors in the twin towers”** (National Commission on Terrorist Attacks 2004, 321).
7. **“The FDNY chiefs would have benefited greatly had they been able to communicate with [police] personnel in a helicopter”** (National Commission on Terrorist Attacks 2004, 321).

E. **Public Information**

1. **“Because of damage to building systems caused by the impact of the plane, public-address announcements were not heard in many locations”** (National Commission on Terrorist Attacks 2004, 286).
2. **“Several South Tower occupants called the Port Authority police desk in 5 WTC. Some were advised to stand by for further instructions; others were strongly advised to leave”** (National Commission on Terrorist Attacks 2004, 289).

F. **Incident Management**

1. **“Several other units self-dispatched . . . . Many off-duty firefighters responded from firehouses separately from the on-duty unit”** (National Commission on Terrorist Attacks 2004, 297).
2. **“While checking floors, they [plainclothes NYPD officers] used office phones to call their superiors. In one phone call an NYPD chief instructed them to leave the North Tower, but they refused to do so”** (National Commission on Terrorist Attacks 2004, 302).
3. **“Some firefighters in the North Tower were off-duty and did not have radios”** (National Commission on Terrorist Attacks 2004, 307).
4. **“FDNY personnel in the North Tower who received the evacuation orders did not respond uniformly. . . . Some units . . . delayed or stopped their evacuation in order to assist non-ambulatory civilians . . . Some units began to evacuate but, according to eyewitnesses did not hurry . . . Other firefighters continued to sit and rest on floors while other companies descended past them and reminded them that they were supposed to evacuate”** (National Commission on Terrorist Attacks 2004, 308-309).

5. **“One of the firefighters apparently heard an evacuation order on his radio, but responded in a return radio communication, “We’re not . . . coming out!”** (National Commission on Terrorist Attacks 2004, 310).
6. **“Redundant searches of specific floors and areas were conducted”** (National Commission on Terrorist Attacks 2004, 321).
7. **“It is equally clear, however, that the Incident Command System did not function to integrate awareness among agencies or to facilitate interagency response”** (National Commission on Terrorist Attacks 2004, 321).

G. **Other**

1. **“There was no backup site” [for the Office of Emergency Management’s Emergency Operations Center]** (National Commission on Terrorist Attacks 2004, 284).
2. **“Some units couldn’t find the staging area”** (National Commission on Terrorist Attacks 2004, 300).
3. **“The primary Field Comm van had access to the NYPD’s Special Operations channel (used by NYPD Aviation), but it was in the garage for repairs on September 11. The backup van lacked that capability”** (National Commission on Terrorist Attacks 2004, 302).
4. **“While significant problems in the command and control of the PAPD also were exposed on September 11, it is less clear that the Port Authority has adopted new training exercises or major incident protocols to address these shortcomings”** (National Commission on Terrorist Attacks 2004, 320).
5. **“The lesson of 9/11 for civilians and first responders can be stated simply: in the new age of terror, they – we – are the primary targets. The losses American suffered that day demonstrated both the gravity of the terrorist threat and the commensurate need to prepare ourselves to meet it”** (National Commission on Terrorist Attacks 2004, 323).

III. **In short:**

- A. **“There have been no standards for domestic incident response that reach across all levels of government and all emergency response agencies” (FEMA IS-700, 2004).**
  - B. **“Responders need to be able to work together, communicate with each others, and depend on each other” (FEMA IS-700, 2004).**
  - C. **“The events of September 11 have underscored the need for and importance of national standards for incident operations, incident communications, personnel qualifications, resource management, and information management and supporting technology (FEMA IS-700, 2004).**
- 

**Objective 34.2      Identify the goals of the National Incident Management System (NIMS).**

Present the following as a lecture:

- I. **Aware of the problems identified by the 9/11 Commission, President George W. Bush issued two Homeland Security Presidential Directives. One called for a National Incident Management System and the other reiterated the importance of disaster preparedness.**
- II. **HSPD-5 was issued on February 28, 2003, and stressed the need to “enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.”**
  - A. **This Presidential Directive:**
    - 1. **Treats crisis management and consequence management “as a single, integrated function, rather than as two separate functions.”**
    - 2. **Encourages the integration of local, state and federal disaster responses.**
    - 3. **Seeks to coordinate government activities with the private and non-profit sectors.**
    - 4. **Promotes information sharing with the public, the private sector, State and local authorities, Federal departments and agencies.**
    - 5. **Provides for improved interoperability and compatibility among local, state and federal capabilities.**

6. **Recommends the development of a National Response Plan.**

III. **HSPD-8** was issued on December 17, 2003, and **had the intention of establishing “policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic attacks, major disasters and other emergencies.”**

A. **This Presidential Directive:**

1. Requires the development of a national domestic **all-hazards preparedness goal**.
2. Ensures **continuous efforts to prepare first responders** for major events – especially for the prevention of and response to terrorist attacks.
3. Describes the **allocation of funds** to states to strengthen capabilities **based on population concentrations, critical infrastructures, and other risk factors**.
4. Points out that the Federal government will **support** state and local entities’ in **planning, interoperability and equipment acquisition**.
5. Establishes **national standards** for preparedness and a multi-year **system of exercises** to test programs.
6. Develops a **system to collect, analyze and disseminate lessons learned, research and best practices** to improve emergency response operations.
7. **Maintains adequate teams, stockpiles and caches** in accordance with national preparedness goals.
8. Encourages **active citizen participation** in preparedness measures.
9. Demands **periodic assessment of progress made and areas needing improvement**.

IV. **The National Incident Management System (NIMS) was created with the goals of these Presidential Directives in mind.**

---

**Objective 34.3      Define the National Incident Management System (NIMS) and mention the principles under which it operates.**

Present the following as a lecture.

- I.      According to FEMA’s independent study course, NIMS “**is a comprehensive, national approach to incident management that is applicable to all jurisdictional levels and across functional disciplines.**”
    - A.      “The **intent** of NIMS is to:
      1.      **Be applicable across a full spectrum of potential incidents and hazard scenarios, regardless of size or complexity.**
      2.      **Improve coordination and cooperation between public and private entities in a variety of domestic incident management activities.**”
  - II.     “**NIMS provides a framework for interoperability and compatibility by balancing flexibility and standardization.**
    - A.      **NIMS provides a flexible framework that facilitates government and private entities at all levels working together to manage domestic incidents. This flexibility applies to all phases of incident management, regardless of cause, size, location, or complexity.**
    - B.      **NIMS provides a set of standardized organizational structures, as well as requirements for processes, procedures, and systems designed to improve interoperability” (FEMA IS-700, 2004).**
- 

**Objective 34.4      Discuss the components of the National Incident Management System (NIMS).**

Present the following as a lecture:

- I.      The **National Incident Management System** is a **framework** to help the nation **prevent, prepare for, respond to and recover from domestic incidents.** It includes **six key components.**
  - A.      **Command and Management.**
    1.      NIMS is based on **three organizational systems.**

- a. The **Incident Command System**, which defines the management structure and operating characteristics at the scene of a disaster or emergency.
  - This may include **unified command**, which includes more than one responding agency or multiple jurisdictions.
  - It may likewise incorporate **area command**, which oversees the management of multiple incidents (that each require ICS organization).
- b. **Multi-agency Coordination Systems**, which define the organizational structure and management principles for those working with or supporting incident command.
  - Such systems **facilitate logistics, allocate resources, track resources, share information, and coordinate interagency and intergovernmental issues regarding policies, priorities and strategies.**
  - These may be **Emergency Operations Centers** and **Multi-agency Coordination Entities** that take a strategic perspective and provide support to incident and area commanders.
- c. **Public Information Systems**, which include processes and procedures for communicating timely and accurate information to the public during emergency situations.
  - Such systems include **Public Information Officers** that advise Incident Command about public information matters.
  - It also includes **Joint Information Centers** where PIOs from multiple agencies meet to provide critical information, crisis communications and public affairs functions.

B. **Preparedness.**

1. Under NIMS, “**preparedness is implemented through a continual cycle of planning, training, equipping, exercising, evaluating, taking action and taking action to correct and mitigate**” (FEMA IS-700, 2004).

2. Preparedness **involves all levels of government and the public and non-profit sectors.**
3. Such readiness efforts are **based on standards and certification** for planning, training, equipment, mutual aid, emergency assistance compacts, etc.
4. Preparedness efforts **require the involvement of “a wide variety of committees, planning groups” to create plans, integrate activities, promote interoperability, establish priorities and improve coordination.**

C. **Resource Management.**

1. “Resource management involves the **coordination and oversight of personnel, tools, processes and systems** that provide incident managers with timely and appropriate resources during an incident” (FEMA IS-700, 2004).
2. It involves **four primary tasks:**
  - a. **Describing, inventorying, requesting and tracking resources.**
  - b. **Activating those systems prior to, during and after an incident.**
  - c. **Dispatching resources prior to, during and after an incident.**
  - d. **Deactivating or recalling resources during or after an incident.**
3. It operates under **five key principles:**
  - a. **Advanced planning** among agencies before disaster strikes.
  - b. **Resource identification** and ordering (using standard processes and methods)
  - c. **Resource categorization** based on size, capacity, capability, skill or other characteristics.
  - d. **Use of agreements** for resources before an incident occurs.

- e. **Effective management**, implying the reliance on validated practices.

D. **Communications and Information Management.**

- 1. NIMS recognizes that **responses require effective communications and information management.**
  - a. This is facilitated by “**a common operating picture** that is accessible across jurisdictions and agencies” (FEMA IS-700, 2004).
  - b. It is also fostered through **common communication terminologies, processes and standards.**

E. **Supporting Technologies.**

- 1. NIMS **recognizes the importance of technology** as long as there is:
  - a. **Interoperability and compatibility**, suggesting that systems must work together.
  - b. **Technology support**, implying that technology is vital in response.
  - c. **Technology standards**, meaning that common rules will enhance interoperability.
  - d. **Broad-based requirements**, conveying the idea that all types of technology, procedures, protocols and standards have been recognized and incorporated.
  - e. **Strategic planning and R&D**, signifying that an agenda for technological research and development has been identified and prioritized.

F. **Ongoing Management and Maintenance.**

- 1. In order to **provide strategic direction, routine review and continual refinement of NIMS**, the **Department of Homeland Security** has **established** a National Incident Management System **Integration Center.**

2. The National Integration Center will be **located in the Federal Emergency Management Agency** and will **serve as a resource** to better coordinate responses to all types of disaster incidents.
- 

**Objective 34.5 Determine the strengths and weaknesses of the National Incident Management System.**

Present the following in a class discussion:

- I. **Divide the students into groups** of 5-6 students.
- II. Ask them to **discuss their thoughts** on the **strengths** and **weaknesses** of NIMS.
- III. After 10 minutes, **ask each group to report their findings**.
- IV. The professor may want to **reiterate the following strengths and weaknesses** during the discussion:
  - A. **Strengths**
    1. **Illustrates learning from 9/11.**
    2. Suggests the need to focus on **all hazards**.
    3. Recognizes the need to **include the public, private and non-profit sectors**.
    4. Desires to **address each phase of emergency management**.
    5. Promotes **proactive** measures for **preparedness**.
    6. Wants to **improve** interagency **communications**.
    7. Gives extra **attention** to **resource management**.
    8. Recognizes the need for **flexibility** and **standardization**.
    9. Is based on the proven Incident Command System
    10. **Updates emergency management** in the United States.
  - B. **Weaknesses**
    1. Illustrates **over-learning** from the 9/11 events.

2. Has an evident **bias toward terrorism**.
  3. Tends to **discuss government operations** more than the public and non-profit sectors.
  4. May **downplay mitigation and recovery**.
  5. **Does not give sufficient attention to prevention activities**.
  6. **Focuses too heavily on technology** for improved coordination.
  7. Possibly **marginalizes functions other than resource management**.
  8. May **stress standardization at expense of flexibility**.
  9. The **Incident Command System** of NIMS may not adequately capture a strategic perspective.
  10. **Reinvents the wheel?**
- 

**Questions to be asked:**

2. **Why was there a need for the National Incident Management System?**
  3. **How did 9/11 affect the development of NIMS?**
  4. **What Presidential Directives affected the direction of NIMS?**
  5. **What are the goals and principles of NIMS?**
  6. **What are the components of NIMS?**
  7. **What are the strengths and weaknesses of NIMS?**
-

---

## **Problems Identified in the 9/11 Commission Report**

---

- Communications Technology
- Communications Procedures
- Information Management
- Interorganizational Coordination
- Public Information
- Information Management
- Other

---

## **NIMS Definition**

---

**NIMS is a comprehensive, national approach to incident management that is applicable to all jurisdictional levels and across functional disciplines.**

---

## **NIMS Components**

---

- **Command and Management**
- **Preparedness**
- **Resource Management**
- **Communications and Information Management**
- **Supporting Technologies**
- **Ongoing Management and Maintenance.**

---

# NIMS Strengths and Weaknesses

---

## Strengths

- Illustrates learning from 9/11
- Suggests the need to focus on all hazards
- Recognizes the need to include the public, private and non-profit sectors
- Desires to address each phase of emergency management
- Promotes proactive measures for preparedness
- Wants to improve interagency communications
- Gives extra attention to resource management
- Recognizes the need for both flexibility and standardization
- Is based on the proven Incident Command System
- Updates emergency management in the United States

## Weaknesses

- Illustrates over-learning from the 9/11 events
- Has an evident bias toward terrorism and away from other types of disasters
- Tends to discuss government operations more than the public and non-profit sectors
- May downplay mitigation and recovery
- Does not give sufficient attention to prevention activities
- Focuses too heavily on technology for improved coordination
- Possibly marginalizes functions other than resource management
- May stress standardization at expense of flexibility
- The Incident Command System of NIMS may not adequately capture a strategic perspective
- Reinvents the wheel?