DISTRICT OF COLUMBIA
EMERGENCY MANAGEMENT AGENCY

National Incident Management System (NIMS)
Implementation Plan

August 2, 2006

Due to the compilation of potentially sensitive data, this NIMS Implementation Plan is marked FOR OFFICIAL USE ONLY (FOUO). As such, anyone wishing to disseminate this document outside of the Local Government should contact the District of Columbia Emergency Management Agency for disclosure review.

Privacy Statement

The disclosure of information in this plan could compromise the security of essential equipment, services, and systems of the District of Columbia or otherwise impart the District' ability to carry out essential emergency responsibilities. Distribution of this NIMS Implementation Plan in its entirety is limited to those who need to know the information in order to successfully activate and implement the plan.

Portions of this plan contain information that raises personal privacy or other concerns, and those portions may be exempt from mandatory disclosure under the Freedom of Information Act.

Any decision to disclose information in this plan outside the District of Columbia or to withhold information in this plan from a non-governmental requester must be coordinated with the District Columbia Office of Emergency Management and with the Office of the Mayor.

Record of Changes

Change No.	Copy No.	Date Entered	Posted By

Recommended changes to this document should be addressed to the
District of Columbia NIMS Compliance Officer

District of Columbia
Emergency Management Agency
National Incident Management System (NIMS) Implementation Plan

TABLE OF CONTENTS

FOREWORD

This document has been developed at the direction of the Mayor of the District of Columbia and in compliance with Homeland Security Presidential Directive (HSPD) 5, *Management of Domestic Incidents*, in which the President directed the Secretary of Homeland Security to develop, submit and administer the National Incident Management System (NIMS). This system will provide a consistent nationwide approach for Federal, State, and Local governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. In like manner, NIMS will provide a consistent approach for the District of Columbia Emergency Management Agency with regard to emergency preparedness, response and recovery.

The NIMS enhances the management of domestic incidents by establishing a single, comprehensive system for incident management and will help achieve greater cooperation among departments and agencies at all levels of government. Implementing the NIMS strengthens DCEMA's capability and resolve to fulfill its responsibilities to all the citizens of the District of Columbia in times of emergency.

The District of Columbia Emergency Management Agency (DCEMA) will serve as the lead District agency for NIMS planning, training, and exercises. The NIMS Implementation Plan is part of the comprehensive "All Hazards" District Response Plan (DRP). The following NIMS Implementation Plan will help ensure that DCEMA has fully incorporated the NIMS into the District of Columbia's emergency response plans, procedures, and policies. The implementation of NIMS will require a demonstrated effort throughout local government. Similar efforts will be required in the private sector.

_____

Barbara Childs-Pair
Director
D.C. Emergency Management Agency

SECTION I: INTRODUCTION

Purpose

This document institutes the necessary steps for compliance with the National Incident Management System (NIMS) implementation plan. This document further ensures that The District of Columbia's Emergency Operations Plan complies with the NIMS; individual domestic incident management; and emergency prevention, preparedness, recovery and mitigation activities, as well as in support of all actions taken to assist regional counter-terrorism task forces and municipal or local municipalities.

Authorities

Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*

Mayor's Order 2005 –146: Adoption of the National Incident Management System

2003 Three-Year Homeland Security Assessment & Strategy and Urban Areas Security Initiatives

References

Homeland Security Act Of 2002.

HSPD-8, *National Preparedness*

DHS *National Incident Management System*, March 1, 2004, U.S. Department of Homeland Security.

DHS, *National Response Plan*, December, 2004.

Scope

This document provides guidance on how the DCEMA plans to implement NIMS.

The provisions of this document apply to all departmental plans, procedures, policies, and training programs, including those fulfilling Emergency Support Functions (ESFs) under the National Response Plan (NRP).

The provisions of this document apply to all sub-components (examples: Agencies, Authorities, Boards, Commissions, Councils, Departments, and Offices), of or operating under the jurisdiction of the District of Columbia (the District or DC).

It is the intent of DCEMA to institute the NIMS as outlined in this document. The timeline for this process is dependent on several factors including staff availability, disaster events, availability of Federal training and exercise programs, Local and Federal Laws and Regulations. Changes in the above could modify the timelines for the implementation of NIMS.

Noncompliance with the NIMS will jeopardize future Homeland Security preparedness funding.

Responsibilities

a. The office of the Mayor is utilizing a decentralized approach to managing emergency events that occur in the District of Columbia. The Emergency Management Agency will meet with agency heads and their senior staff to coordinate planning, training, exercises, and preparedness efforts. The result of this review is to be reported back to the Mayor as required.

b. Agency Directors are responsible to ensure that the following emergency planning and preparedness activities are in place:

1. Designate a Point of Contact (POC) to be the liaison with the EMA staff. See Figure I-2 for a complete listing of Agency Points of Contact.
2. Review agency emergency plans, procedures, and preparedness efforts to confirm that they are fully compliant with the DRP.
3. Agency POC's and/or senior decision makers for each agency shall participate in monthly NIMS implementation meetings.
4. Assign members of the respective agencies to attend NIMS training. This training is directed at agency members who have assigned emergency duties and responsibilities.
5. Ensure that personnel that may be assigned to the Emergency Operations Center (EOC) and other departmental operating centers are trained and fully proficient with current software programs
6. In conjunction with UASI Training & Exercise Manager, ensure that members of each agency participate in emergency training and exercises.
7. Begin development of Continuity of Operations Plan (COOP) that should contain critical information on alternate work sites, restoration of District services, back-up of critical information, line-of-succession, etc.

NIMS Implementation Senior Advisory Committee:

Ronald Gill Jr.	FEMS/EMA	ronald.gill@dc.gov
Christopher Voss	EMA	chris.voss@dc.gov
Cathy Lanier	MPD	cathy.lanier@dc.gov
Lawrence Schultz	FEMS	Lawrence.schultz@dc.gov
Natalie Jones-Best	DDOT	Natalie.jonesbest@dc.gov
Daniel Harrison	DPW	daniel.harrison@dc,gov
Gayle Swain	DOH	g.swain@dc.gov
Dr. Terry Thomas	DHS	terry.thomas@dc.gov
Nabiat.Solomon	DOE	nebiat.solomon@dc.gov
Rhonda Mackabee	OCTO	Rhonda.mackabee@dc.gov

NIMS Implementation Team:

The NIMS implementation Team consists of representatives from the following:

Office of Homeland Security
District of Columbia Emergency Management Agency (DCEMA)
District of Columbia Fire and Emergency Medical Services (DCFEMS)

Metropolitan Police Department (MPD)
District of Columbia Department of Transportation (DDOT)
District of Columbia Department of Health (DOH)
District of Columbia Department of Public Works (DPW)

The NIMS Implementation Team is responsible for:

- Ensuring the District of Columbia fully adopts all components of NIMS.

- Coordination of all agencies and departments, with multi-municipal coordination systems and unified command.

- Development of concepts and principles to institutionalize all-hazards incident management and integration strategies compliant with the National Response Plan (NRP). Including local utilization of NRP and the District Response Plan (DRP).

- Assurance that vertical and horizontal coordination occurs at the local level of government and at the planning and response levels.

- Identifying and updating all training, plans, and programs to fully integrate NIMS concepts and terminology.

- Recommendation of appropriate training levels for all DCEMA personnel and Emergency Liaisons Officers (ELOs).

- Development of a timeline to complete necessary training for all DCEMA personnel and ELOs

- Ensuring NIMS Implementation is in alignment is in alignment with the goals and objectives defined in the 2003 District of Columbia Three-Year Homeland Security Assessment and Strategy and Urban Areas Security Initiatives including participation and concurrence of stakeholders.

Each department/agency is to designate a point of contact person with a key role in implementing NIMS who will serve as the key contact for DCEMA regarding all NIMS implementation correspondence. Departments/Agencies must provide contact information to Ronald Gill, NIMS Compliance Officer at ronald.gill@dc.gov or (202) 673-2101 ext. 1173.
Table I-2 identifies key contact information.

Position Title	Point of Contact	Office Telephone	Responsibilities to Ensure Full Adoption of the NIMS
Emergency Management Director	Barbara Childs-Par	(202) 673-2101 ext.1165	Oversight of compliance and implementation efforts
Emergency Management Deputy Director	Mark Brown	(202) 673-2101 ext.1156	Oversight of Emergency Planning and NIMS compliance
NIMS Compliance Officer	Ronald Gill Jr.	(202) 673-2101 ext.1173	Chair of NIMS Compliance Planning Team, manage implementation
Emergency Planner	Chris Voss	(202) 673-2101 ext. 1141	EOP revisions and COOP development
UASI Training	Brian Baker	(202) 673-2101 ext.1198	Schedule and manage NIMS training
UASI Exercises	Jamie Quarrelles	(202) 673-2101 Ext.1223	Schedule and manage NIMS exercises
WebEOC	Josh Jack	(202) 673-2101 ext. 1193	WebEOC program development

Table I-1. Identification of Key Personnel

Organization	POC	Alternate POC
Child and Family Services Agency		
Department of Consumer and Regulatory Affairs		
Department of Fire & EMS		
Department of Health		
Department of Housing & Community Development		
Department of Human Services		
Department of Motor Vehicles		
Department of Parks & Recreation		
Department of Public Works		
Department of Transportation		
DC Housing Authority		
DC Public Schools		
Emergency Management Agency		
Metropolitan Police Department		
Office of Chief Medical Examiner		
Office of the Chief Technology Officer		
Office of Contacting & Procurement		
Office of Energy		
Office of Planning		
Office of Property Management		
Office of Tax and Revenue		
Office of Unified Communications		
Office of Zoning		
DC Public School		
Office of Contracting and Procurement		

Table I-2 Identification of Agency Points of Contact

SECTION II: CONCEPT OF IMPLEMENTATION

II-1. The Phases of NIMS Adoption

The NIMS adoption for the District of Columbia will include seven distinct phases. These implementation phases will overlap in order to speed and strengthen the process. All District agencies must achieve NIMS implementation by the end of FY 2006. Table II-1 illustrates the expected NIMS implementation timelines based on phase descriptions below for DCEMA and all District departments/agencies.

DCEMA will revise this Plan to reflect all Federal DHS and NIMS compliance requirements. DCEMA will provide departments/agencies with ongoing guidance relative to compliance issues. Additionally, DCEMA will post pertinent NIMS project information on the DCEMA website.

Phase One consists of the formal recognition of NIMS and adoption of NIMS principles and policies.

Phase Two consists of employee training (see Section III: Employee Training). This will also include completion of the FEMA's Emergency Management Institute courses on the NIMS IS-700, ICS-100, and ICS-200. In addition to that training, supervisory personnel will also be required to complete IS-800. More training for supervisory personnel is forthcoming in 2007. All supervisors with responsibility over operational assets will be accountable for ensuring that all employees are fully trained in the NIMS. All agencies must also incorporate NIMS into current training programs where appropriate.

Phase Three will include of the establishment of a NIMS baseline by using the NIMS Capability Assessment Tool (NIMCAST). All agencies will utilize the NIMSCAST to establish baselines to determine NIMS requirements already met. Completion of this survey is expected to be on or around August 1, 2006. The results of this survey will be sent to the NIMS Compliance Officer for review. A second, final assessment will be completed by all agencies and forwarded to NIC via the NIMS Compliance Officer. The final assessment will be sent no later than September 22, 2006.

Phase Four consists of NIMS compliance documentation (also see Section V: Compliance Documentation). All agencies and affected personnel have been directed to maintain their own records regarding training and other compliance related issues. Other compliance documentation should include changes made to existing plans, procedures, and policies to make them NIMS compliant, as well as development, execution, and after-action documentation for any training that occurs to validate the integration of NIMS into various agencies.

Phase Five calls for the evaluation and modification of existing plans, policies, and procedures to identify aspects in need of augmentation for NIMS compliance. In particular, the District Response Plans (DRP) and the Continuity of Operations Plans (COOP) must be evaluated for NIMS incorporation. All agencies must also integrate resource typing and the certification and credentialing of both equipment and personnel into departmental plans, procedures, and policies (refer to Section VIII: Resource Management). More information on credentialing and resource typing can be found at www.fema.gov/emergency/nims/mutual_aid.shtm.

Phase Six consists of departmental/agency verification of achievement of the NIMS Integration Centers (NIC) standards (also see Section VIII: Verification of NIC Standards Achievement). DCEMA and all District agencies will conduct and/or participate in exercises to demonstrate compliance with NIMS Integration Center standards. In particular, DCEMA will conduct operational exercises involving District agencies to demonstrate NIMS compliance.

Phase Seven consists of the institutionalization of the ICS by all District departments/agencies. The institutional use of the ICS is critical to the success of a department's/agency's ability to manage large scale incidents.

Actions to institutionalize the use of ICS take place at two levels – policy and organizational/operational. At the policy level, ICS must be adopted by executive order, proclamation, or legislation and incident managers and response organizations must be directed to train and exercise using ICS.

At the organizational/operational level, institutionalizing ICS into departments/agencies requires internal policies and procedures. Training must be planned and underway. Responders at all levels must be participating in and/or coordinating ICS-oriented exercises that involve responders from multi-disciplines and jurisdictions. The disciplined use of ICS in day-to-day operations is the only way to assure effective ICS when transitioning to incidents of a large scope that require complex incident management. The level that ICS is institutionalized can be noted in the NIMSCAST baseline.

II-2. NIMS Adoption Timetables

The list below summarizes NIMS implementation phase information. The number of months correlate with the number of months it will take DCEMA and other District agencies to complete each phase. The timetables shown in Tables II-1 and II-2 begin September 2005 and continue to the end of FY 2006 when Federal DHS requires full NIMS compliance.

Phase I – Formal Recognition of NIMS and Adoption of NIMS Principles and Policies (All agencies) — **Completed**

a. Mayor's Order on September 30, 2005

Phase II – Employee Training (All agencies) — **11 months**

a. ICS-100 – Introduction to Incident Command System
b. ICS-200 – Basic Incident Command System
c. IS-700 – National Incident Management System
d. IS-800 – The National Response Plan
e. Other relevant courses (to be determined)
f. Internal training/tabletop exercises

Phase III – NIMS baseline (ALL agencies) — **2 months**

a. NIMSCAST final report (All agencies) — **4 months**

Phase IV – NIMS Compliance Documentation **in progress**

a. NIMS Compliance Tracking agency data entry

Phase V – Modification of Relevant Plans, Procedures, and Policies **13 months**

a. Emergency response plans, including those that fulfill Emergency Support Functions under the NRP and internal response plans, such as COOP and the DRP must be modified to adopt NIMS principles and language.
b. Develop/enhance/modify training programs to institutionalize NIMS.
c. Process includes modification, testing, refinement, and implementation.
d. Agencies must integrate resource typing and the certification and credentialing of both equipment and personnel into departmental plans, procedures, and policies).

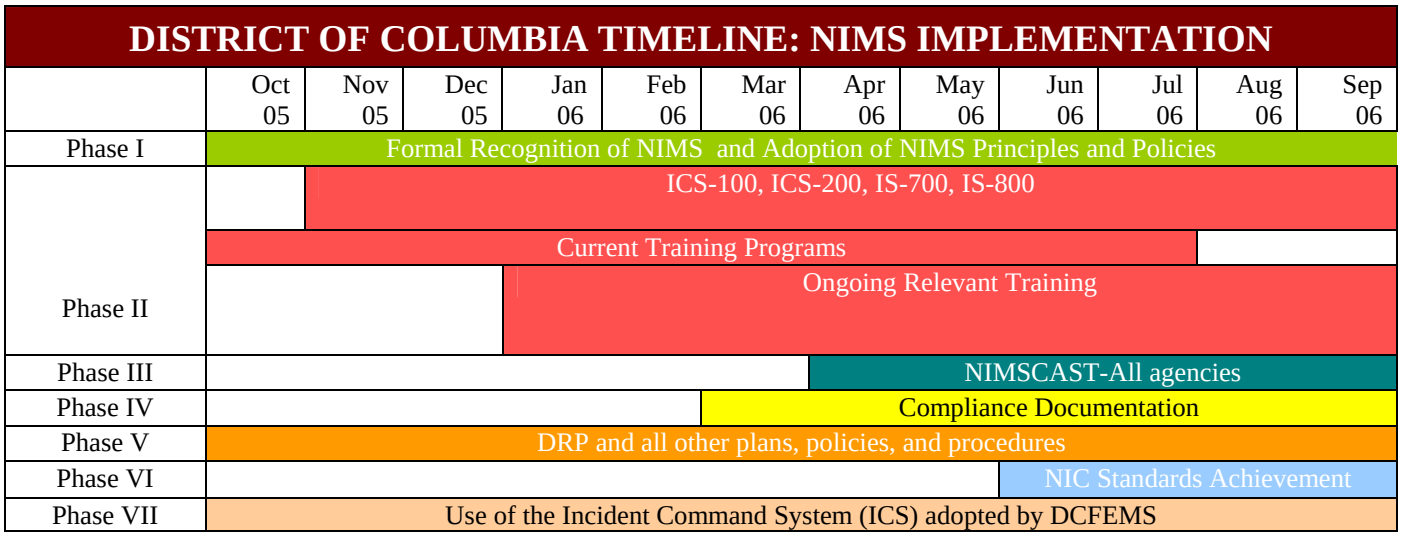
Phase VI – Verification of NIC Standards Achievement **ongoing**

a. Validation exercises.
b. Certification and credentialing of employees (further guidance on both are forthcoming).

Phase VII – Use of the Incident Command System (ICS) **Completed**

	COMPONENT
Phase I	Formal Recognition of NIMS and Adoption of NIMS Principles and Policies
Phase II	Staff Training
Phase III	NIMS Baseline
Phase IV	Compliance Documentation
Phase V	Modification of Relevant Plans, Procedures, and Policies
Phase VI	Verification of NIC Standards Achievement
Phase VII	Use of the Incident Command System (ICS)

Following this schedule will ensure the City meets the September 2006 deadline for NIMS adoption.



Fiscal Year 2006

Table II-1. Expected NIMS Implementation Timeline

SECTION III: STAFF TRAINING

III-1. Staff Training

Phase Two of NIMS implementation consists of staff training. The table in this section identifies current NIMS compliance training requirements. DCEMA will update this table as Federal DHS issues further NIMS implementation training requirements. Departmental personnel with responsibility over NIMS training requirements must ensure all employees in theirs respective departments/agencies complete NIMS training requirements, in addition to incorporating NIMS into all current training programs where appropriate. Individual departments/agencies may conduct and/or participate in additional meetings, training, and exercises to facilitate NIMS compliance. Departments/agencies must document all NIMS-related training as proof of compliance (See Section Five: NIMS Compliance Documentation).

III-2. Identification of Required Training Components

The Department is encouraged to use the following tables to identify the training employees will receive relevant to NIMS implementation. The courses listed are recommended. The first table reflects the training requirements for all Departmental employees and the second the training requirements for all employees with additional emergency response duties.

The following table illustrates the training **ALL** employees with emergency response duties, those that are subject to work at the Emergency Operations Center (EOC) or those that will be reassigned from their current work location to one of the previously mentioned situations will receive relevant to NIMS implementation, including internal/regional training, such as tabletop exercises. Additionally, support personnel from any District agency or department that would be deployed during or following a significant event or in support of the District or an individual agency continuity of operations plan (COOP) should have the listed training in Figure III-1.

Training Course/Internal Training	Expected Completion Date
IS-100, Introduction to the ICS	September 30, 2006
IS-200, Basic ICS	September 30, 2006
IS-700, NIMS an Introduction	September 30, 2006

Table III-1. Training Requirements for All Employees with emergency response related duties

Figure III-2 illustrates the training all employees with duties that directly or indirectly involve or support all hazard **incident management** will receive relevant to NIMS implementation, including internal/regional training, such as tabletop exercises. This includes District Agency/Department heads and their designees that may have a role in the District Response Plan, or any personnel that may be assigned to duties in the EOC.

SECTION III: STAFF TRAINING

Training Course/Internal Training	Expected Completion Date
IS-100, Introduction to the ICS	September 30, 2006
IS-200, Single Resources	September 30, 2006
IS-700, NIMS an Introduction	September 30, 2006
IS-800, National Response Plan (NRP)	September 30, 2006
ICS-300	2007
ISC-400	2007

Table III-2. Training Requirements for employees with emergency response duties and supervisory roles

III-3. Incorporation of NIMS into Current Training Programs

In addition to new training requirements, departments and agencies must enhance and modify current training programs to permanently incorporate NIMS and ensure ongoing NIMS education.

Departments/agencies must review current training programs involving emergency preparedness, incident management, and response to determine if NIMS incorporation is necessary. Federal DHS may further dictate specific training programs departments/agencies must modify. Departments/agencies will identify all such programs and develop a NIMS incorporation strategy. Departments/agencies are to document all training, exercises, and other events related to the incorporation of NIMS into current training programs as proof of compliance (see Section Five: NIMS Compliance Documentation).

SECTION IV: NIMS BASELINE

IV-1. NIMS Baseline

Phase three consists of the establishment of a NIMS baseline. All District of Columbia departments/agencies that fall under the NIMS umbrella will complete a NIMCAST Assessment. This will assist those agencies in developing a baseline to determine the current status of their respective department's incident preparedness against the requirements outlined in NIMS. Baselines will assist departments/agencies in determining additional actions and resources necessary to effectively implement NIMS.

IV-2. NIMCAST

a) Departmental/Agency Requirements.

NIMCAST is a web-based self-assessment tool designed to aid local jurisdictions in determining present capabilities and compliance against Federal DHS-established NIMS requirement. Agencies will utilize the NIMS Capability Assessment Support Tool (NIMSCAST) to establish departmental/agency baselines.

b) Department/Agency Designee.

All agencies will assign one designee to complete NIMSCAST prior to the deadline. The appointed designee should be a staff member most familiar with NIMS and ICS. Designees may view the online demo to familiarize themselves with assessment categories and questions. If necessary, the appointed designee may collect feedback from other departmental/agency personnel tasked to provide input on the department's/agency's incident management capabilities. Once all necessary information is gathered, the appointed designee must complete the online tool.

c) NIMCAST Access.

NIMCAST is available on the Federal Emergency Management Agency's (FEMA) NIMCAST website at http://www.fema.gov/nimcast/index.isp. The NIMCAST User's Guide is available online and maybe accessed from FEMA's NIMSCAST website or it maybe accessed directly from the following address: http://www.fema.gov/nimscast/img/pdf/NimcastUsersGuide.pdf. The online user's guide provides users will step-by-step instructions on using NIMCAST.

d) NIMCAST Structure.

NIMCAST currently encompasses Chapters II through VI of the NIMS document

- Command and Management
- Preparedness
- Resource Management
- Communication and Information Technology
- Supporting Technologies

NIMS Chapters II through I include compliance requirements. NIMCAST is a compilation of these NIMS compliance requirements in a "Yes/No" question format. Several NIMCAST questions include information providing help or clarification for answering that particular question.

To complete NIMSCAST, users simply click on the chapter and section they would like to complete. NIMSCAST automatically saves all data input by the user's baseline assessment. NIMSCAST takes users approximately one hour to complete online assessment.

e) NIMCAST Permissions.

There are two types of NIMCAST accounts: public and official. Official NIMSCAST accounts are permission-based, that is, users must first be "invited" to create an official account. Departments/agencies required to complete NIMSCAST must first create a public account outside the official permission-based system at this time.

f) Submitting Baseline Data.

Users, when invited, will establish 'official' accounts for their assessment jurisdiction. NIMSCAST links all baseline data to the jurisdictional accounts, not the users. Even if the NIMS Manager removes or reassigns the user, the data entered remains in the system.

Baseline data entered into public accounts does not become accessible by any jurisdiction until users transfer that data into an official account.

Once users transfer baseline data into the official account, users must then submit the baseline data results by using the "Submit for Rollup" link. Users "roll up" baseline data results to the next highest account level. Users cannot change submitted data.

g) NIMSCAST Versions.

NIMSCAST allows users to save up to six versions of the assessment, including a baseline version (optional). When users complete an assessment, NIMSCAST will prompt users to name the version. Users may then create additional versions. Users can replace older with newer ones and delete existing versions. However, users cannot delete the initial baseline version. Multiple versions allow users to compare assessment results and track NIMS implementation progress.

SECTION V: COMPLIANCE DOCUMENTATION

V-1. Compliance Documentation

NIMS compliance documentation will be handled at the agency level. Personnel should contact their individual agency training coordinator for assistance with documentation. Agencies should have a central point of contact for NIMS training documentation. All affected employees are strongly encouraged to maintain personal records as well.

For non-training related compliance activities, it is recommended that agency Points of Contact (POC) assure that all NIMS related activities are well-documented for future review. Specifically, documentation should capture all existing plans, policies, and procedures as they exist today and modifications made to them to assure compliance. Additionally, any training conducted should be well-documented from exercises conception through after-action. This should include deficiencies found and how those items were corrected in your agency plan.

SECTION VI: MODIFICATION OF PLANS, PROCEDURES, AND POLICIES

VI-1. Modification strategy of Plans, Procedures, and Policies

Phase Five of NIMS implementation consists of departmental modification of existing plans, policies, and procedures requiring modification and finalization to reflect full NIMS adoption. DCEMA and all other departments/agencies will identify all such, plans, policies, and procedures and may utilize Tables VI-1 and VI-2, respectively, to assist in developing a NIMS incorporation strategy and identifying targeted milestone dates.

In particular, DCEMA will evaluate and revise the Emergency Operations Center Standard Operating Procedures (EOC SOP) and the District Response Plan (DRP). All other departments/agencies will evaluate and revise SOPs for NIMS incorporation. Other department/agency emergency response plans in support of NRP and any internal emergency plans will also require revision.

Departments/Agencies must first identify existing plans, policies, and procedures in need of modification for NIMS compliance. Modification also consists of testing, refinement, and implementation. Additionally, all departments/agencies must enhance and modify relevant training programs associated with these plans, procedures, and policies. Section III-3 addresses the incorporation of NIMS into current training programs.

VI-2. NIMS Emergency Operations Plans Guidance

Emergency Operations Plans (EOP) provides a comprehensive framework for emergency management of all hazards. U.S. Department of Homeland Security NIMS Guidance points out the need for state and local plans to be coordinated with the National Response Plan principles and language. By September 30, 2006, state and local agencies must modify existing incident management and emergency operations plans to ensure proper alignment with the NRP coordinating structures, processes, and protocols. To that end, the District of Columbia is organized into sixteen (16) Emergency Support Functions (ESF's) and several support and incident annexes in alignment with the NRP.

NIC will release a NIMS EOP template to assist all departments/agencies with plan revision and finalization. DCEMA will notify all departments/agencies when NIC releases this template.

Table VI-3: NIMS EOP checklist (NIMS, Chapter III, Section B) illustrates the status of NIMS incorporation into department/agency EOPs. Departments/agencies may utilize this checklist in conjunction with the NIC EOP template, to revise and finalize respective SOPs and EOPs identified in Section VI-1

An integral part of a complete set of plans includes a Continuity of Operations Plan (COOP). COOP planning is designed to develop and maintain a plan that enables each jurisdiction to preserve, maintain, and/or reconstitute its capability to function effectively in the event of the threat or occurrence of any disaster or emergency that could potentially disrupt government operations and services. A basic COOP plan outlines provisions to ensure continuity of government authority and the order of succession for key positions; identify the key personnel to perform essential functions in an emergency; develop strategies for protecting vital records, databases, systems, and equipment; and identify, evaluate, and select the alternate facilities to be used for the organization's emergency operations.

EOP Title _____	Checklist	Adoption Date
Defines the scope of preparedness and incident management activities necessary for the jurisdiction.	☐	
Describes organizational structures, roles, and responsibilities, policies, and protocols for providing emergency support.	☐	
Facilitates response and short-term recovery activities	☐	
Is flexible enough to use in all emergencies.	☐	
Describes the EOP purpose.	☐	
Describes the EOP situation and assumptions.	☐	
Describes the EOP concept of operations.	☐	
Describes the EOP organization and assignment of responsibilities.	☐	
Describe the administration and logistics of the EOP.	☐	
Describes EOP Development and maintenance.	☐	
Describe the EOP authorities and references.	☐	
Contains functional annexes.	☐	
Contain hazard-specific appendices.	☐	
Contains a glossary.	☐	
Pre-designates jurisdictional and/or functional area representatives to the Incident Commander (IC) or Unified Commander (UC) whenever possible.	☐	
Includes pre-incident and post-incident public awareness, education, and communications plans and protocols.	☐	

Table VI-2. NIMS-Compliant EOP Checklist

SECTION VII: RESOURCE MANAGEMENT

VII-1. NIMS Resource Management

In addition to plan modification, Phase Five also addresses NIMS resource management. Resource management consists of: (1) resource typing; and (2) certification and credentialing of employees.

VII-2. Resource Typing

NIMS emphasizes the importance of maintaining accurate and up-to-date information on resource management as a critical component of domestic incident management. FEMA's National Mutual Aid and Resource Management Initiative serves as the basis to type, inventory, order, and track Federal, State, and local assets. This initiative supports equipment and personnel compatibility necessary for mutual aid agreements. Resource typing definitions for 120 of the most common response resources are available at: www.fema.gov/nims/mutualaid.shtm.

Federal DHS bases NIMS on the need for standard definitions and practices. Differing definitions will in effect negate the fundamental idea that all responders should be using common definitions when ordering or receiving assets through mutual aid. Systems that do not conform to these common definitions are not compliant with NIMS.

By September 30, 2006, departments/agencies should integrate resource typing into modified response plans, procedures, and policies. DCEMA will update this Section to reflect further guidance fro Federal DHS. All departments/agencies should develop and update its resource inventories in accordance with typed definitions. For resources not yet typed by Federal DHS, departments/agencies will define resources by capacity and capability in accordance with Federal DHS-established resource typing methodology. Up-to-date response asset inventories are critical for effective NIMS implementation.

Table VII-1 indicates the strategy and timeframe for developing or updating a comprehensive inventory of response resources.

Department/Agency Name	Strategy for Resource Inventory Development	Timeline for Completion
DCEMA	Pending	To be determined
All Departments/Agencies	Pending	To be determined

Table VII-1. Strategy and Schedule for Developing a Resource Inventory

VII-3. Certification and Credentialing of District of Columbia Employees and Equipment

The creation of a nationwide credentialing system is a fundamental component of the NIMS and the National Mutual Aid and Resource Management initiative. This system recognizes the availability and the capability of response personnel and equipment, including qualifications, certifications, and accreditations. This system will reinforce state-to-state relationships in existing mutual aid systems. In addition, a national credentialing system will incorporate existing standards of all disciplines into a "national standard". This will allow the nation to adopt a uniform credentialing system that facilitates immediate and routine identification and dispatch of appropriate and qualified personnel and equipment resources to any incident. The credentialing initiative will focus initially on the following disciplines:

- Emergency Management
- Firefighting/ Search and Rescue
- Emergency Medical Services
- Hazardous Materials Response
- Law Enforcement
- Health Care
- Public Health
- Public Works

NIC will expand its NIMS Curriculum in the future to include training established to meet national credentialing standards. DCEMA will update this Section and Section II: Staff Training to reflect national credentialing standard requirements.

In the foreseeable future, a working group will began developing a standard for credentialing personnel and equipment. Realizing several jurisdictions have begun building ID/credentialing systems, every effort will be made to incorporate this data into the global solution.

Departments/agencies will integrate employee and equipment certification and credentialing into modified response plans, procedures, and policies. DCEMA will update this Section to reflect further guidance from Federal DHS. Table VII-2 indicates the strategy and timeframe for certification and credentialing of personnel and equipment.

Department/Agency	Strategy for Certification/ Credentialing Development	Timeline for Completion
DCEMA	Pending	To be determined
All District Departments/Agencies	Pending	To be determined

Table VII-2. Strategy and Schedule for Certification/Credentialing Development

SECTION VIII: VERIFICATION OF NIC STANDARDS ACHIEVEMENT

Phase Six consists of the verification of the District of Columbia's support and achievement of the NIMS Integration Center (NIC) standards. Federal DHS has tasked NIC with validating national compliance with NIMS and NRP responsibilities, standards, and requirements. At present, States will be self-certifying. DCEMA will update this Section to reflect further guidance from Federal DHS regarding NIC standard compliance validation.

Until NIC releases further guidance on validation, the District of Columbia will continue to conduct exercises to verify achievement of NIC standards. DCEMA has conducted several local exercises during FY2006 to demonstrate NIC standards compliance and will continue to do so through FY2007. The NCR has conducted several Operational Area and region-wide exercises during the past year to demonstrate NIC standards compliance and will continue to do so through FY 2006. The District of Columbia designs and implements all exercises according to Federal DHS-developed methodology and guidance of the Homeland Security Exercise and Evaluation Program (HSEEP).

ANNEX A: GLOSSARY OF KEY TERMS

A more comprehensive listing of non-District of Columbia key terms can be found by clicking on the NIMS Document or NRP Document.

District of Columbia specific Key Terms are listed below:

Assessment: The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Emergency: Absent a Presidentially-declared emergency, any incident(s) human-caused or natural, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.

Emergency Operations Centers (EOCs): The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (fire, law enforcement, and medical services), by jurisdiction (Federal, State, county, city, tribal), or some combination thereof.

Emergency Operations Plan: The "steady-state" plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

Emergency Response Provider: Includes Federal, State, local, and tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities. See Section 2 (6), Homeland Security Act of 2002, Pub L. 107-296, 116 Stat. 2135 (2002). Also known as *Emergency Responder.*

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

Federal: Of pertaining to the Federal Government of the United States of America.

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

Incident: An occurrence or event, natural or human caused that requires an emergency response to protect the life or property. Incidents can, for example, include major disasters, emergencies, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Incident Commander: The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

Incident Management Team (IMT): The IC and the appropriate Command and General Staff personnel assigned to an incident.

Joint Information Center (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media at the scene of the incident. Public information officials from all participating agencies should collocate at the JIC.

Jurisdiction: 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 (city, county, tribal, State, or Federal boundary lines) or functional (law enforcement, public health).

Local Government: A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. See Section 2 (10), Homeland Security Act of 2002, Pub L. 107-296, 116 Stat. 2135 (2002).

Major Disaster: As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, tribes, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Mitigation: The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures, often formed by lessons learned from prior incidents involve ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

Multi-agency Coordination Systems: Multi-agency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The components of multi-agency coordination systems include facilities, equipment, emergency operation centers (EOCs), specific multi-agency coordination entities, personnel, procedures, and communications. These systems assist agencies and organizations to fully integrate the subsystems of the NIMS.

Multi-jurisdictional Incident: An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents are managed under Unified Command.

Mutual-Aid Agreement: Written agreement between agencies and/or jurisdictions that they will assist one another on request, by furnishing personnel, equipment, and/or expertise in a specified manner.

National: Of a nationwide character, including the Federal, State, local, and tribal aspects of governance and policy.

National Incident Management System: A system mandated by HSPD-5 that provides a consistent nationwide approach for state, local, and tribal governments; the private-sector, and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among state, local, and tribal capabilities, the NIMS includes a core set on concepts, principles, and terminology. HSPD-5 identifies theses as ICS; multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

National Response Plan: A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.

Non-governmental Organization: An entity with an association based on interests of its members, individuals, or institutions and not created by a government, but may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross.

Preparedness: The range of deliberate, critical tasks and activities necessary to build sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training, and exercises, personnel qualification and certification, equipment certification, and publication management.

Prevention: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agriculture surveillance and testing processes; immunizations, isolations, and quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Private Sector: Organizations and entities that are not part of any governmental structure. It includes for-profit organizations, formal and informal structures, commerce and industry, and private voluntary organizations (PVO).

Processes: Systems of operations that incorporate standardized procedures, methodologies, and functions necessary to provide resources ordering and tracking, and coordination.

Qualification and Certification: This subsystem provides recommended qualification and certification standards for emergency responder and incident management personnel. It also allows the development of minimum standards for resources expected to have an interstate application. Standards typically include training, currency, experience, and physical and medical fitness.

Recovery: The development, coordination, and execution of service-and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

Recovery Plan: A plan developed by State, local, or tribal jurisdiction with assistance from responding Federal agencies to restore the affected area.

Resources: Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at the EOC.

Resource Management: Efficient incident management requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under the NIMS includes mutual-aid agreements; the use of special state, local, and tribal teams; and resource mobilization protocols.

Response: Activities that address the short-term, direct effects of an incident. Response includes immediate action to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations to determine the full nature and source of the threat; public health and agriculture surveillance and testing processes; immunizations, isolations, and quarantine; and, as appropriate, specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity and apprehending actual perpetrators and bringing them to justice.

Standard Operating Procedure: Detailed, written instructions to achieve uniformity in the performance of a specific function.

State: When capitalized, refers to 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. See Section 2 (14), Homeland Security Act of 2002, Pub L. 107-296, 116 Stat. 2135 (2002).

Supporting Technologies: Any technology that is used to support NIMS is included in this subsystem. These technologies include orthophoto mapping, remote automatic weather stations, infrared technology, and communications, among various others.

Tribal: Any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaska Native Claims Settlement Act (85 stat. 688) [42 U.S.C.A. and 1601 et seq.], that is recognized as eligible for the special program and services provided by the United States to Indians because of their status as Indians.

Type: A classification of resources in the ICS that refers to capability. Type 1 is generally considered to be more capable than types 2, 3,3or 4 respectively, because of size; capacity; in the case of incident management teams, experience and qualifications.

Unified Command: An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single Incident Action Plan (AIP).

WebEOC: A software package that is specifically designed for incident management, incident generated records management, and resource tracking. This software in use in many localities throughout the country.

ANNEX B: TRAINING REQUIREMENTS

COLOR CODE: **AWARENESS = GREEN** **OPERATIONAL = BLUE** **SUPERVISORY = YELLOW** **COMMAND = RED**	**ICS-100 Introduction to the ICS**	**EMI IS-700 NIMS**	**EMI IS-800 National Response Plan**	**ICS-200 Level Course or Equivalent**	**ICS-300 Intermediate Level Course or Equivalent**	**ICS-400 Advanced ICS**
Firefighters						
Police officers						
Emergency medical services providers						
Public works on-scene personnel						
Public health on-scene personnel						
First line supervisors						
Single resource leaders						
Lead dispatchers						
Field supervisors						
Company officers and entry level positions (trainees) on Incident Management Teams						
Other emergency personnel that require a higher level of ICS training						\

COLOR CODE: **AWARENESS = GREEN** **OPERATIONAL = BLUE** **SUPERVISORY = YELLOW** **COMMAND = RED**	**EMI IS-100 Introduction to the ICS**	**EMI IS-700 NIMS**	**EMI IS-800 National Response Plan**	**ICS-200 Level Course or Equivalent**	**ICS-300 Intermediate Level Course or Equivalent**	**ICS-400 Advanced ICS**
Middle Management						
Strike Team Leaders						
Task Force Leaders						
Unit Leaders						
Division/Group Supervisors, Emergency Liaison Officers (ELO)						
Branch Directors and Multi-Agency Coordination System/Emergency Operations Center Staff						

COLOR CODE: **AWARENESS = GREEN** **OPERATIONAL = BLUE** **SUPERVISORY = YELLOW** **COMMAND = RED**	**EMI IS-100 Introduction to the ICS**	**EMI IS-700 NIMS**	**EMI IS-800 National Response Plan**	**ICS-200 Level Course or Equivalent**	**ICS-300 Intermediate Level Course or Equivalent**	**ICS-400 Advanced ICS**
Command and general staff						
Agency Administrators						
Department Heads						
Emergency Managers						
Area Commander and Multi-Agency Coordination System/Emergency Operations Center managers						
Elected officials; senior executives; senior managers; and agency administrators with policy responsibilities, but without specific ICS or Multi-Agency Coordination System function/roles or responsibilities						

As a rule of thumb, in the unlikely event of an emergency, if you will be supporting the response effort, first responders, answering phone, planning, logistics, operations, and/or administrative functions, law enforcement, Fire, Emergency Medical Services, elected officials and/or transportation, you are required to take at a minimum the IS-100 Basic Incident Command System and the IS-700 National Incident Management System Awareness courses.