NIMS GUIDELINE FOR THE CREDENTIALING OF PERSONNEL

DRAFT
NOVEMBER 21, 2008

TABLE OF CONTENTS

OVERVIEW

The National Incident Management System (NIMS) *Guideline for the Credentialing of Personnel* (the *Guideline*) establishes recommended protocols to facilitate the coordinated response to incidents. These incidents can range from large-scale terrorist attacks to catastrophic natural disasters that require interstate deployable mutual aid. The *Guideline* is intended to encourage interoperability among Federal, State, and local officials and will facilitate deployment for response, recovery, and restoration. This *Guideline* also will allow incident commanders to exercise enhanced access control in times of crisis.

The *Guideline* is intended to enable emergency response officials to spend less time processing and being processed and more time responding to the incident. For non-Federal stakeholders called in to support mutual aid, the *Guideline* will help ensure that emergency response officials from multiple jurisdictions and sectors will have interoperable processes. The implementation of processes based on the *Guideline* will also benefit the owners and operators of critical infrastructure and key resources (CIKR) and other private-sector entities by establishing and communicating protocols for access based on affiliation to enable early restoration of their own facilities and services.

The *Guideline* is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across jurisdictions and to establish a common approach to disaster response across the Nation. It describes specific authority and best practices for managing interstate disasters and integrates the credentialing process within the Incident Command System (ICS).

The most important application of the *Guideline* is for response to disasters requiring interstate mutual aid. As currently developed, this document uniquely informs domestic emergency management mutual aid initiatives. While not developed as such, the *Guideline* could also serve to inform international cross-border mutual aid initiatives undertaken by States. Given the nature of disasters of this kind, all partners will be needed. Attaining trust, coordination, and cooperation among all is critical for success.

INTENDED AUDIENCE

The *Guideline* is written especially for government executives, CIKR owners and operators, private-sector and nongovernmental organization (NGO) leaders, and emergency management practitioners. First, it is addressed to senior elected and appointed leaders, such as Federal department and/or agency heads, State Governors, mayors, tribal leaders, and city and/or county officials—those who have a responsibility to provide effective response.

Second, it explains to private-sector entities affected by the disaster which procedures to follow for entering the impacted area to carry out their own response and recovery activities within the ICS.

Third, the *Guideline* informs emergency management practitioners by explaining the credentialing and typing processes and tools used routinely by Federal Emergency Response Officials (FEROs) and emergency managers at all levels of government. For these users, the *Guideline* is augmented with online access to supporting documents, further training, and an evolving resource for exchanging lessons learned.

PURPOSE OF CREDENTIALING

The purpose of credentialing is to ensure and readily validate the identity and attributes (such as affiliations, skills, or privileges) of an individual. Credentialing is critical to the incident management community so it can plan for, request, and trust resources needed for emergency assistance, receive personnel resources that match requests, and appropriately manage officially dispatched responders. The *Guideline* provides core information to be used by all response organizations, including operational definitions for important terms and the key credentialing processes.

The purpose of credentialing is to ensure that the incident management community can plan for, request, and trust resources needed for emergency assistance, receive personnel resources that match requests, and appropriately manage officially dispatched responders. The *Guideline* provides core information to be used by all response organizations, including operational definitions for important terms and the key credentialing processes.

Many of the functions and processes of credentialing and affiliation access should exist prior to an incident and be ongoing throughout the incident response. (See Section 1 for a checklist of these recommended functions and processes.) However, many States have existing processes and systems to allow for compliance with these recommendations while producing "just-in-time" credentialing at the moment of actual deployment. Nothing in this *Guideline* should be construed as preempting States from executing just-in-time credentialing.

It is the intent of the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) to improve emergency management and response capabilities in the United States for all major disasters, emergencies, and other incidents where interstate mutual aid is required. To achieve this, DHS and FEMA recognize the existing authority for States to regulate mutual aid within their borders and seek to build on the States' existing processes and systems to improve the delivery of interstate mutual aid. This *Guideline* does not preempt or diminish the sovereignty of the States to manage response operations in accordance with their laws.

NIMS CREDENTIALING

The benefit of implementing NIMS credentialing is that it provides confidence that the personnel and resources provided match the request; both parties, requester and supplier, are using the same criteria to identify knowledge, skills, and abilities. This confidence alleviates one concern from communities already struggling with the effects of a disaster. However, in order for this system to work it is imperative that the basic principles of identity, qualification/affiliation, and invitation are embraced and utilized.

Developing a culture of NIMS credentialing is also important so that when an event occurs, the response is disciplined and the adverse effects of an unauthorized deployment are avoided.

GUIDELINE

The *Guideline* presents the key credentialing and typing principles, participants, roles, and structures that guide the Nation's credentialing operations, by expanding on the fundamental principles established in NIMS Guide 0002 and explaining how credentialing efforts within the United States can work under NIMS and ICS. Additionally, it addresses a process for affiliation access for CIKR that facilitates entry for those organizations that are essential to the overall response and restoration but are not direct participants in mutual aid or government-led incident management activities. The remainder of the *Guideline* covers the following topics:

- **Section 1** – Characteristics of credentialing and physical access control systems
- **Section 2** – State and local governments and the Emergency Management Assistance Compact (EMAC)
- **Section 3** – Affiliation access for private businesses and organizations, including those that manage and serve the Nation's critical infrastructure
- **Section 4** – Voluntary and other nongovernmental organizations, including charities, faith-based organizations, and other not-for-profit entities
- **Section 5** – The Federal Government and its authorized contractors

SECTION 1 – CHARACTERISTICS OF NIMS CREDENTIALING AND AUTHORIZED ACCESS

This section describes the principal characteristics recommended to States and local authorities for their consideration in adopting policies to enable credentialing and access control for responders and recovery personnel deployed to an incident area. *While these processes are voluntary, following them will strengthen eligibility for Federal grants supporting preparedness by aligning State and local policies and procedures with NIMS.*

The purpose of NIMS credentialing is to establish a national definition and recommended criteria for credentialing as they relate to personnel, including those ordered as single resources or assigned to teams, as well as crew assigned to equipment or those listed within the "Tier One" NIMS national resource typing definitions as posted by the NIMS Integration Center. For the purposes of NIMS, the term credentialing refers to information a person will present to the requesting jurisdiction—i.e., (1) identity, (2) qualification/affiliation, and (3) authorization for deployment. NIMS credentialing does not confer the authority or privilege to practice any profession. Only the receiving jurisdiction can extend that privilege or authority after evaluating the person's information.

CREDENTIALING VS. AFFILIATION ACCESS

This *Guideline* recognizes the need for processes to address the full range of access control, both for individuals who provide the resources, skills, and competencies to support the incident command structure and for those who require access for specific purposes outside of the NIMS/ICS purposes.

The NIMS credentialing process supports resource typing for government responders and supporting capabilities, and works best when the participating individuals (affiliation and skills) can be preidentified.

These processes do not necessarily apply to the restoration of CIKR facilities and services, as the CIKR owners and operators are responsible for identifying the needed skills and competencies of response personnel and validating the qualifications of their own repair crews or service providers. However, CIKR owners and operators cannot accurately preidentify contracted response personnel and resources. Therefore, this *Guideline* details an affiliation access process that encourages State and local leaders to develop processes that are based on affiliation with an identified CIKR facility or system.

BEST PRACTICES FROM THE DHS CREDENTIALING FRAMEWORK

The credentialing lifecycle is comprised of six phases. "Credentialing," as used in this report, is the entire process of determining a person's eligibility for a particular license, privilege, or status, from application through issuance, use, and expiration or potential revocation of the issued credential. The phases are:

- Registration and Enrollment.

- Eligibility Vetting and Risk Assessment.

- Issuance.

- Verification and Use.

- Expiration and Revocation.

- Redress/Waiver.

All credentialing programs should seek to incorporate best practices common to each of the credentialing phases including interoperable verification technologies. To assist its partners in managing these investments in credentialing programs, DHS established the Credentialing Framework Initiative (CFI). The CFI is intended to guide investments that will improve programs' ability to meet their missions by:

- Creating a consistent security risk-based framework across the credentialing lifecycle, that can be used to improve our ability to achieve national security goals and objectives.

- Supporting an interoperable architecture, improving reuse of information technology (IT) services.

- Improving credentialing processes through eliminating redundant activities and leveraging investments across programs, reducing costs of implementing new capabilities as well as the costs of supporting some of the credentialing capabilities.

- Improving the experience for individuals applying for credentials.

- Ensuring personally identifiable information (PII) is protected and used consistent with the purpose for which it was collected.

DHS has identified several core problems common to credentialing programs that may be solved by incorporating desired characteristics.

Core Problem	Desired Characteristic
Inefficient information and data collection	Enrollment platforms and data collection investments so that they can be reused by other programs where appropriate—establishing a preference for an "enroll once, use many" environment.
Multiple credentials for an individual	Credentials to support multiple licenses, privileges, or status based on the risks associated with the environments in which they will be used.
Inconsistent vetting processes for like programs and re-vetting of the same individuals	Vetting, associated with like uses and like risks, should be the same.
Reliance on visual inspection	Entitlement to a license, privilege, or status should be verified using technology.
Data collection or processing errors	Opportunities for redress—individuals should be able to correct information held about them.

For more information, please refer to the Credentialing Framework Initiative available from the DHS Screening Coordination Office by contacting FEMA-NIMS@dhs.gov.

IMPLEMENTING NIMS CREDENTIALING

The credentialing process is voluntary and applies to first responders who would be deployed under interstate mutual aid agreements or compacts. In order for the first responder to be credentialed, the department or agency that employs the first responder would need to agree to participate in the process. There are two levels of participation, and each department or agency determines its own level.

- Level 1: Personnel and teams to be deployed as a single resource
- Level 2: Personnel and teams to be deployed as part of a response team as defined in existing and deployable interstate response resources or assets

NOTE: If the resources or assets are not available or not adequate to fulfill the mission requirements, the participation of that department/agency will cease.

Once the department/agency determines its level of participation and identifies the personnel and teams with appropriate knowledge, skills, and abilities, the personnel or team application(s) are submitted to the authorized credentialing agency for approval. If it is determined that the submitted personnel are not qualified, the application(s) will be denied and the individuals or teams have the option to reapply.

If the individual or team applications are approved, the credentialing organization will, at a minimum:

1. Create a record and update its database.

2. Notify the department/agency of the credentialing decision.

3. Issue (and periodically reissue) an ID card.

4. Record the information in a management infrastructure.

5. Arrange for periodic review of the credentialing process by a third-party reviewer.

NIMS CREDENTIALING CHECKLIST

The following checklist covers the functions and processes that make up credentialing:

• Establish standards for the jobs and duties of emergency response officials from minimum through advanced levels or degrees of competency.

• Process individuals' and organizations' requests to become credentialed.

• Provide education, training, and experience that supports individuals in achieving and maintaining a credential or credentials.

• Verify the individual's competency in knowledge, skills, and abilities required to meet the performance standards for which a credential is sought or maintained.

• Verify the individual's health and fitness as indicated for the credential and the duties to be performed.

• Establish processes for canceling, withdrawing, and revoking credentials electronically, respecting due process and establishing a process for appeal.

• Perform monitoring and quality control of the organizations that credential, verify, and select emergency response officials and recovery personnel.

• Audit and test the relevant organizations, including the accrediting organizations involved in these credentialing processes and functions.

• Conduct and support research and testing of the credentialing system and the effectiveness of credentialing in meeting its purposes.

The following checklist covers the activities for the office receiving the personnel:

• Plan for credentialed and noncredentialed personnel needs before and during an incident.

• Request personnel resources and transmittal processes performed under NIMS/ICS (relating to the use of credentialed and noncredentialed personnel).

• Receive and process requests.

• Issue invitations to organizations or individuals based on requests.

- Determine and disseminate the processes for security and access controls for an incident, including the "rules of engagement" to be applied to credentialed emergency response officials who have been officially requested and sent, or deployed by incident/unified commands, and for affiliate-access purposes. (These rules should also clarify what to do with those who are unauthorized or cannot properly establish their identity.)

- Establish check-in processes for credentialed personnel and for affiliate-access purposes to include the checking of identification, credentials, and authorizations.

- Report incident experiences and lessons learned related to deployed personnel and their credentials or related to the credentials they may be seeking.

- Report adverse events reflecting on a person's credentials.

The following checklist covers responsibilities for the office sending requested personnel to an incident:

- Verify identity and the person's credential prior to sending them. (This applies to just-in-time and short-notice requests for mutual aid.)

- Issue authorization documentation to the emergency response officials and recovery personnel who are to be sent.

- Transmit lists of personnel being sent to a requesting jurisdiction.

- Deploy emergency response officials and recovery personnel, and manage them using resource-tracking protocols.

- Maintain rosters and electronic databases of deployed individuals.

SECTION 2 – STATE/LOCAL GOVERNMENT, TRIBAL NATIONS, AND THE EMERGENCY MANAGEMENT ASSISTANCE COMPACT

This section is intended to assist State and local governments and tribal nations in amending or adopting laws that would conform to the *Guideline* for the purpose of enhancing response from the private sector, volunteer organizations, and other State, tribal, and local governments.

The Federal Government recognizes that success during any disaster or emergency depends on the laws and powers being exercised by State, tribal, and local governments and that powers are extensive and independent of the Federal Government. Nothing in this *Guideline* should be interpreted as preempting States, tribes, or local governments from exercising their legal authorities to manage response and recovery operations within their jurisdictions.

Tribal governments are sovereign nations. As such, they are encouraged to review their existing rules and laws that apply to NIMS and ICS and to revise them in accordance with the recommendations provided in this document. If tribal governments credential personnel in specific conformity with the *Guideline*, the credentialed person will be recognized by all Federal agencies and State and local governments that have adopted the same guidance.

Credentialing is expected to provide substantial benefits to tribal governments by assisting them in making requests for mutual aid and in deciding whether to respond to a request or invitation to provide personnel resources. Tribal nations, along with all governments and organizations in the United States, should benefit from using the credentialing guideline provided in this document.

GENERAL GUIDANCE

The *Guideline* is not a call for States, tribes, or local governments to overturn existing credentialing, licensing, or board certification laws, or the way these existing processes and procedures are implemented. Any change to existing laws or processes are entirely a matter of State, tribal, or local policy.

In order to comply with the *Guidelines*, State governments, in conjunction with local and tribal governments, are urged to:

- Designate a credentialing authority empowered by the State for overall management of the credentialing functions and processes.
- Determine how the State will work with other levels of government within the State and with tribal nations to implement the *Guideline*.
- Determine how the credentialing function will be implemented (i.e., how each of the disciplines and various emergency response groups will be credentialed and which agencies and/or organizations will be authorized to perform the processes expected).
- Determine a process to facilitate access for CIKR and other entities that are not subject to the credentialing requirements. This process should be based on affiliation.
- Establish a program for issuing credentials for interstate mutual aid incidents.
- Maintain a registry or database of all typed or credentialed personnel.

- Credential and type their employees who have emergency response skill sets.

- Provide verification of credentials upon receiving proper inquiries.

- Develop an implementation process that ensures the credentialing activity is maintained and supports both preincident and short-notice credentialing situations.

- Provide for a situation in which any job, duty, or credential is not addressed in State regulations.

- For those entities that will be using technology to enable credentialing, consider interoperability with FIPS 201 as an end-state objective to allow for incorporation of common standards and a common trust framework. However, this is not a requirement.

GRANT INFORMATION RELATED TO THE *GUIDELINE*

All Federal agencies who make preparedness grants should allow State, tribal, and local governments to use these funds to implement the *Guideline,* per NIMS Guide 0002. Nothing in this *Guideline* requires any State, tribal, or local government to implement this *Guideline* for mutual aid delivered exclusively within their jurisdictional borders.

EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC)

All 50 States and territories have enacted laws agreeing/conforming to EMAC. States may form compacts that will have legal standing and jurisdiction if given the consent of the Congress.[1] The Federal Government recognizes that EMAC may issue rules and adopt processes and services in addition to those listed in this *Guideline*.

The following should be followed whenever EMAC is invoked:

- Any person properly requested, invited, and authorized for deployment under EMAC should be considered credentialed and typed to serve the role for which he or she is deployed.

- State and local officials are to provide support and assistance to ensure that a person credentialed under EMAC can reach an appropriate incident check-in site or process.

- Unless directed otherwise by the incident/unified command, security and access controls should not unreasonably detain an individual credentialed and authorized to deploy for mutual aid under EMAC. This guidance also applies to the accompanying team authorized to deploy with the individual (affiliate-access). If security and access control has the identity of the individual and the authenticity of the EMAC documentation, the responding individuals, team, and resources are to be processed and assisted to reach check-in sites or processes as quickly as possible.

---

[1] Examples include international arrangements such as Public Law 110–171, the International Emergency Management Assistance Memorandum of Understanding (IEMAMOU) between the U.S. States of Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut and the Canadian Provinces of Quebec, New Brunswick, Prince Edward Island, Nova Scotia, and Newfoundland; and Public Law 105–381, the Pacific Northwest Emergency Management Arrangement (PNEMA) between the U.S. States of Alaska, Idaho, Oregon, and Washington and the Canadian Provinces of British Columbia and the Yukon Territory.

- Unless the incident/unified command or the jurisdiction having authority establishes rules specific to the incident, disaster, or emergency, the identity of a person is established by: 1) documentation in accordance with the Real ID Act; 2) two photo IDs; or 3) a photo ID and the official EMAC documentation.

- States are encouraged to establish credentialing and typing processes that include critical infrastructure personnel as well as those who work for volunteer or charitable organizations and their accompanying teams.

As part of EMAC's continuous improvement in collaboration with FEMA, mission packages are being developed to expedite deployments of fully capable teams. These teams are based on the Typed Resources and include properly qualified personnel. This enhancement should be integrated into EMAC operations by all States as follows:

1. States should build mission packages (also called pre-scripted missions) by resource type, capabilities, skills, equipment, personnel, logistical needs, limitations, and cost resources that could be shared through interstate mutual aid.

2. When a mission package is requested, the State emergency management agency assigns, invites, and authorizes personnel for deployment under EMAC. Such personnel should be considered credentialed to serve in the role for which they are deployed.

3. Personnel under EMAC should report to the requesting State staging area with their State-issued identification, government-issued identification, and EMAC mission documentation. States could issue an event or site identification card that would serve, during the mission, as their authorization to be at the event.

4. Personnel would then be allowed to conduct their mission.

5. Personnel would check out at the staging area upon demobilization.

SECTION 3 – AFFILIATION ACCESS FOR THE PRIVATE SECTOR AND CRITICAL INFRASTRUCTURE AND KEY RESOURCES

GENERAL GUIDANCE

The purpose of this section is to provide guidance for developing and implementing access control and affiliation documentation for personnel restoring CIKR. Access control will augment the standardized process for credentialing and resource typing according to NIMS, while recognizing the unique responsibilities of private-sector CIKR owners and operators to manage and oversee the restoration of facilities and services.

This section defines the essential characteristics of access control procedures for CIKR personnel and equipment preparing for, responding to, or recovering from the effects of a natural or manmade disaster. Adopting these guidelines will bring State, local, tribal, and regional jurisdictions into alignment with NIMS Guide 0002. Voluntary alignment with NIMS Guide 0002 facilitates Federal grants and other funding mechanisms to assist Federal, State, and local preparedness planning.

As defined by the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 (HSPD-7) of December 2003, as well as recent revisions, the Nation's CIKR includes the following sectors: 1) Agriculture and Food; 2) Defense Industrial Base; 3) Energy (including oil, gas, and electric power, except for commercial nuclear power facilities); 4) Public Health and Healthcare; 5) National Monuments and Icons; 6) Banking and Finance; 7) Water (including drinking water and water treatment systems); 8) Chemical; 9) Commercial Facilities; 10) Dams; 11) Emergency Services; 12) Nuclear Reactors, Materials, and Waste; 13) Information Technology; 14) Communications; 15) Postal and Shipping; 16) Transportation Systems (including air, rail, road, maritime, and mass transit); 17) Government Facilities; and 18) Critical Manufacturing.

The vast majority of the Nation's CIKR is owned and operated by the private sector, which has responsibility for determining the resources and personnel required to respond and recover. In many incidents requiring emergency management and response, CIKR facilities are damaged or their services disrupted. The repair of these facilities and the restoration of essential services are among the most important steps in returning the community to normalcy. The process for affiliation access applies to those private-sector entities that do not derive a benefit from government-oriented credentialing protocols.

Implementing an access control process to enable more rapid private-sector CIKR response and restoration efforts provides numerous benefits for overall incident management and response efforts. The two overarching goals of establishing an access control process for CIKR are:

- To enable CIKR owners and operators to quickly restore their affected facilities.

- To support the core NIMS principles of flexibility and standardization by encouraging State and local authorities to adopt a common approach to affiliation access for private-sector CIKR.

ACCESS CONTROL AND AFFILIATION DOCUMENTATION

Access control provides a process for identifying and providing services to CIKR entities that are located in the affected area and a process for including these entities in phased reentry planning. It also enables them to designate recovery personnel, employees, contractors, and/or equipment to enter an incident area. Affiliation documentation provides the identification these personnel need to gain access to an incident area.

Access control and affiliation documentation processes will be used by CIKR owners and operators to deploy the personnel and equipment needed to restore their facilities and services within an incident area based on a timeline deemed appropriate by incident command. Since the CIKR within an incident area normally falls within State and/or local jurisdictions, processes for access control and affiliation documentation should be administered by the States or delegated to local authorities.

IMPLEMENTATION GUIDANCE FOR AFFILIATION ACCESS

It is recommended that States develop and provide an access control process that can be quickly implemented during disaster response and recovery. The process should:

- Support and facilitate execution of Federal, State, tribal, and local responsibilities and authorities.
- Ensure that appropriate authorities grant priority access to personnel, crews, and equipment needed for CIKR damage assessment and restoration before, during, and after an incident.
- Ensure that access decisions, identification requirements, and, if appropriate, credentials are communicated and recognized at all levels of access control.
- Enable processes that will support advance identification and authorization of CIKR entities, when practical. For example, it may be advisable to provide the appropriate affiliation documentation or credentials to certain known CIKR officials who will require access for damage assessments. However, it most likely is not practical to know in advance the full range of personnel and equipment that will be called in for CIKR facility or service repair and restoration.
- Ensure that the most efficient methods of identification verification are applied. For those entities that will be using technology to enable credentialing, interoperability with FIPS 201 should be considered as an objective to foster common standards and a common trust framework. However, this is not a requirement.
- Ensure that processes are consistent for State, local, and private-sector constituencies.

It is recommended that States and local authorities consider the following in developing access control within their jurisdictions. This program should:

- Work within the overall Incident Command System.
- Support effective and responsive decisionmaking.

- Clearly define points of contact within State and local government, the ICS, and the private sector that have decisionmaking responsibilities for access control.

- Identify an individual or position within the jurisdiction's incident management or governance structure responsible for ensuring authorized CIKR access and responding to requests for information and appeals for access.

- Clearly define the documentation process for authorized CIKR representatives/recovery personnel, their equipment, vehicles, convoys, and/or supplies to gain access to a controlled site.

- Recognize that CIKR owners and operators are responsible for identifying personnel and equipment needed to protect or restore their facilities, assets, or services within the incident area.

- Be definable, recognizable, efficient, and effective.

- Provide a framework for consistency and interoperability across multiple jurisdictions.

- Be easy to implement.

- Be flexible and responsive to accommodate all contingencies.

- Allow response personnel/resource sequencing or a tiered approach to reentry to an incident area.

- Support personnel and equipment access for corporate/company resources, as well as contractors who may be hired by CIKR owners and operators.

- Encourage preincident credentialing and typing and preincident documentation for recognized CIKR within a given jurisdiction.

- Be administered from within the controlling jurisdiction.

- Provide for effective and timely communication of the required processes and documentation to all jurisdictions and agencies controlling access, including law enforcement, emergency management, and the National Guard.

- Focus on meeting CIKR needs for fast, efficient, and smooth priority access to their facilities, systems, and networks.

- Provide for local discretion to expedite access and bypass requirements under certain conditions.

- Encourage local jurisdictions to adopt interoperable access control systems.

- Be incorporated in National, regional, State, tribal, and local exercises to ensure that emergency management at all levels, and CIKR within given jurisdictions, are aware of the program and begin to include it in their preparedness planning.

It is recommended that States and local authorities consider the following for affiliation documentation within their jurisdictions. This documentation should:

- Allow for invitation by a recognized valid CIKR entity.

- Allow for preapproval and registration for recognized CIKR within the jurisdiction to permit expedited access to an incident area if necessary.

- Allow authorized CIKR officials to distribute access control documents to response and recovery personnel/employees and contractors under certain conditions.

- Use an electronic validation process.

- Identify a centralized source for tags, invitation letters, or other documentation.

- Be clearly identifiable (photo ID, company ID) but not too complex or diverse to cause access delay.

- Allow admittance by large travel teams, such as convoys, with minimal delay.

- Allow for on-site distribution of access credentials for crews already on scene.

- Ensure that the authorizing jurisdiction proactively communicates affiliation documentation to CIKR owners and operators within the jurisdiction well in advance of any incident.

- Be communicated to local law enforcement, emergency response officials, and all other Federal, State, and local agencies likely to respond to an incident.

- Allow for regular review and improvement through lessons learned from events and exercises.

- Be supportable and executable across a range of contingencies and incidents of all sizes and complexities.

SECTION 4 – VOLUNTARY, CHARITABLE, AND NOT-FOR-PROFIT ORGANIZATIONS

GENERAL GUIDANCE

The purpose of this section is to provide guidance on the credentialing and typing of personnel who may be deployed in response to a disaster. Voluntary, charitable, and not-for-profit organizations, including faith-based organizations, provide response/recovery personnel and other resources during a disaster. Credentialing and typing can benefit these organizations by standardizing terms and providing minimum guidelines for personnel to be assigned to an emergency/incident scene.

Organizations are encouraged to seek the assistance of the respective State, tribal, and local governments to ensure consistency and compliance with their requirements and to integrate with the credentialing processes established in conformance with the *Guideline.* Individuals who are officially requested, invited, authorized, credentialed, and typed are more likely to reach the emergency check-in points. State, tribal, and local governments may issue conforming credentials for the employees or volunteers of these organizations.

Adopting practices that will work in concert with credentialing as defined in the *Guideline* will integrate the organization's response/recovery personnel into the established incident command processes and facilitate critically needed response. To conform to the *Guideline*, these organizations are encouraged to:

• Assist their personnel in obtaining and maintaining credentials that conform to the *Guideline*.

• Ensure that individuals have proper identification in addition to a credential.

• Establish processes for responding to invitations/requests for assistance and for providing authorizations and documentation for their responders/response personnel.

• Maintain a roster or database of credentialed personnel to match the requests for interstate mutual aid with the resources and responders of the organization.

• Develop and maintain processes to assist inquirers at receiving/security controls and check-in points to validate/verify identities, authorizations, and credentials.

• Provide information to and training for their volunteers and employees about credentialing.

• For those entities that will be using technology to enable credentialing, consider interoperability with FIPS 201 as an end-state objective to allow for incorporation of common standards and a common trust framework. However, this is not a requirement.

Credentialing may be governed by State, tribal, and local laws. All organizations are encouraged to become familiar with these laws, including those pertaining to EMAC. Therefore, individuals who 1) do not have proof of identity, 2) cannot demonstrate they have been requested and officially authorized, or 3) cannot prove they were sent by their owning organizations should be turned away. Furthermore, they may be subject to other actions by the proper authorities.

Nothing in this section or in NIMS Guide 0002 is to be interpreted to encourage, condone, or permit individuals to self-deploy, or to gain access to restricted areas during an emergency, or to hold immunities from tort and other liabilities that arise from their unauthorized actions.

SECTION 5 – CREDENTIALING OF FEDERAL EMERGENCY RESPONSE OFFICIALS (FEROS)

GENERAL GUIDANCE

The purpose of this section is to provide guidance on credentialing and typing of Federal department and agency personnel as FEROs under NIMS. This information is directed to Federal departments and agencies that have defined roles under the National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), or National Continuity Policy Implementation Plan (NCPIP) for executing NIMS credentialing and typing. The goal is an enhanced ability to manage assets during a national incident.

This section defines the additional actions departments and agencies must accomplish to supplement their implementation of HSPD-12/FIPS 201. The additional actions are contained in NIMS Guide 0002.

The four elements of NIMS credentialing and typing are identity, attributes (knowledge, skills, and abilities), deployment authorization, and access control validation. For the purposes of this *Guideline*, identity and access control validation will be documented through the requirements of HSPD-12 and FIPS 201. Attributes are to be determined by departments and agencies based on the assigned roles their personnel will fill within the Emergency Support Function (ESF) or Support Annex structure of the NRF or through their roles as CIKR Sector-Specific Agencies or Government Coordinating Council members as detailed in the NIPP and the CIKR Support Annex to the NRF; and will be electronically assigned, leveraging FIPS 201 credentials issued to FEROs. Deployment authorization must be documented and may take several forms, from mission assignments to deployment orders. However, until sufficient FIPS 201 credential readers are available, separate paper copies of qualifications and deployment authorizations should be issued to FEROs so that the first three elements of NIMS credentialing and typing—identification, qualification/affiliation, and authority to deploy—can be inspected by access control personnel.

A FERO meets the NIMS credentialing and typing requirements only when the first three elements of NIMS are complete. Possession of a FIPS 201 credential is essential but not sufficient to meet NIMS credentialing and typing requirements. A FERO with a proper FIPS 201 credential and proof of qualifications is not NIMS-credentialed unless he or she also has physical possession of an acceptable deployment authorization. Incident managers need to be aware of and authorize assets deployed in order to execute their responsibilities effectively.

IMPLEMENTATION GUIDANCE – IDENTIFICATION

Federal departments and agencies must comply with the requirements of HSPD-12/FIPS 201 to establish the identity of employees and contractors. Federal departments and agencies must identify their personnel who are likely to be deployed in accordance with assignments in the NRF, NIPP, or NCPIP. These personnel will be designated as FEROs, and their FIPS 201 credential visually marked accordingly.

IMPLEMENTATION GUIDANCE – QUALIFICATIONS

The qualifications of FEROs shall be determined by their department or agency, based on the functions and missions these personnel will perform. They will be assigned to:

- The NRF Emergency Support Function under which they will operate;

- The Sector of the NIPP they will support; and/or

- Their National Continuity functions as essential government officials.

It is a requirement that the FERO qualification be electronically integrated with the FIPS 201 credential for credentialing and typing. However, until credential readers are universal, it is a near-term requirement that personnel be issued qualification cards that can be visually inspected by access control officials.

NOTE: A critical component of identity and qualifications is revocation. If a FERO leaves his or her department or agency, his or her identity must be removed from all affected databases within 18 hours as required by FIPS 201. Additionally, if a FERO's qualifications change (additions, deletions, promotions, etc.), the FERO's qualifications must be changed in all affected databases within 18 hours. Revocation of a FERO's identity revokes his or her HSPD-12/FIPS 201 credential in totality. Revocation of or changes to qualifications are reflected when the HSPD-12/FIPS credential is electronically validated, but the agency does not revoke the HSPD-12/FIPS 201 credential itself.

IMPLEMENTATION GUIDANCE – DEPLOYMENT AUTHORIZATION

Each department and agency is responsible for providing FEROs with valid deployment authorization. For NRF deployments, this is typically the mission assignment. For deployments under department or agency authority, it is the travel authorization, clearly stated in the Purpose section.

While a mission assignment or travel authorization meets the needs of Federal facilities such as the Joint Field Office (JFO), it may be necessary to obtain supplemental documentation from State Emergency Operations Centers (EOCs) to validate the State's acceptance of the FEROs for access to the State or the disaster area.

DOCUMENTATION

Each Federal department and agency shall prepare an electronic inventory of all personnel determined to be FEROs, listing their assignment and the ESF or Sector to which they will provide support upon activation. This inventory shall be submitted electronically to the FEMA Assistant Administrator for Disaster Operations not later than October 27, 2008.

Each Federal department and agency shall provide updates to the inventory as required, but at the minimum annually on May 1 to facilitate planning for hurricane season.

GLOSSARY OF TERMS AND DEFINITIONS

Whenever NIMS or ICS is employed within the United States, the following definitions apply:

- **Credentialed** – Describes a person who has in his or her possession *all three* elements outlined in NIMS Guide 0002 (i.e., proof of (1) identity, (2) qualification or affiliation, and (3) authorization for deployment).

  NOTE: Currently the three elements may be presented in physical and/or electronic format (e.g., hard-copy material or data transmitted using technologies). Any elements of credentialing established under EMAC, or under any State or tribal law for the specific intent of complying with this Guideline*, are to be used in the applicable jurisdiction.*

- **Credentialing** – All the administrative processes that result in issuing, using, monitoring, managing, or revoking any or all of the elements necessary for a person to be credentialed (i.e., (1) identity, (2) qualification/affiliation, and (3) authorization for deployment.

- **Check-In** – An incident-specific process (logical or physical) that is established by incident/unified commands to receive individuals and to determine whether they will be granted authorization to be accepted for emergency and incident management, response, or recovery purposes. Credentialed individuals are to be assisted to reach check-in processes established by incident command. This term is not to be used to refer to security and access control situations.

- **Affiliate-Access** – This term refers to the way individuals are to be treated under this *Guideline*. This *Guideline* recognizes that at certain stages of a disaster, teams of people will be arriving at an incident to perform important duties and functions, such as CIKR restoration, but that they may not be credentialed in specific conformance with this *Guideline*. This *Guideline* intends that such individuals be assisted in fulfilling these duties and functions.

- **Affiliation Access** – This term refers to the procedures, systems, and processes devised by States and local authorities to permit CIKR owners and operators to send in repair crews and other personnel to expedite the restoration of their facilities and services in areas affected by a disaster. Affiliation access includes such processes as access control and affiliation documentation for authorized CIKR personnel, contractors, and their equipment.

Credentialing is defined for Federal agencies by this document, HSPD-12, and the documentation supporting FIPS 201. States and tribal nations are encouraged to examine their credentialing authorities and to establish these where necessary to be in conformance with this *Guideline*.

NOTE: No one is required as a result of this Guideline *to be credentialed as defined here, nor does this* Guideline *compel anyone who holds proof of identity and qualification/affiliation to come forward in time of an emergency or disaster (although they may be compelled by other laws or reasons). Emergency response officials and recovery personnel are encouraged to come forward voluntarily to be credentialed, and, when responding to an incident, they are encouraged to follow the processes established in conformance with this* Guideline *by the*

authorities having jurisdiction (e.g., States, local governments, existing mutual aid agreements, and EMAC).

NOTE: Holding proof of identity and qualification/affiliation established under this Guideline *DOES NOT PERMIT an individual to self-deploy to an incident without following this* Guideline *or applicable laws.*

Credentialing supports and facilitates qualified individuals to be requested, invited, sent, received, and employed. Credentialing assists these individuals in gaining access to resources, sites, and/or systems needed to perform their assigned functions, tasks, or duties. Three key processes are essential for these actions to occur and are defined as follows:

- **Identity** – *Is the emergency response official the person he or she presents himself or herself to be?* Verifying identity is an important process critical to the use of a credentialed person in mutual aid response.

- **Request, Invitation, and Authorization** – *Is the emergency response official officially deployed in response to a request for assistance*? Incident/unified commands make requests for resources and personnel. Organizations invite individuals to fill these requests. Once an organization has identified the appropriate personnel, they are provided documentation supporting the specific request.

    EMAC: The documentation issued under EMAC serves to communicate that the response and recovery persons have been sent to the location requesting assistance by a jurisdiction having authority. Under EMAC, a properly identified and qualified person who presents the proper documentation of his or her authorization for deployment shall be considered credentialed for the purposes of this *Guideline*. This *Guideline* recognizes that EMAC may define the processes and rules that are to be applied to their processes for a request, invitation, and authorization.

- **Security and Access** – *Is the emergency response official permitted access?* Incident/unified command determines the rules that permit a person to have access to resources, sites, and/or systems. Being credentialed does not automatically guarantee access. Security and other personnel should be aware of the rules granting access so that appropriate personnel can be permitted swift access where they are needed. If site-specific "badging" approaches are be used, these badges *should not* be referred to as "credentials."

STATUTES

The *NIMS Guideline for the Credentialing of Personnel* is issued to comply with Section 510 of the Homeland Security Act of 2002, as amended (6 U.S.C. 320). The *Guideline* has been developed to establish definitions to explain and identify actions and processes that can provide the foundation for a consistent use and interoperability of credentialing on a national scale for the communities of interest defined herein. Its overall purpose is to strengthen NIMS and ICS to improve emergency management and response within the United States.

The Homeland Security Act as amended contains several new sections to strengthen the use of ICS by establishing a credentialing guideline and guidance affecting Federal agencies and their authorized contractors to assist State, tribal, and local governments, and other emergency response official organizations. Nothing in this *Guideline* is intended to displace or harm the mutual aid agreements that exist or arise within the United States or with its international mutual aid partners.

POINTS OF CONTACT

This *Guideline* is issued by FEMA in accordance with the Homeland Security Act as amended. For more information about this *Guideline* or about credentialing under NIMS and ICS, contact: FEMA National Preparedness Directorate, National Integration Center (NIC), Incident Management Systems Integration Division (IMSI) at FEMA-NIMS@dhs.gov.