NIMS GLOSSARY OF TERMS AND DEFINITIONS

(excerpt from "NIMS Guideline for the Credentialing of Personnel" Draft 11/21/08)

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.”