Designation: E2842 − 14 (Reapproved 2021)

Standard Guide for Credentialing for Access to an Incident or Event Site[1]

This standard is issued under the fixed designation E2842; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

INTRODUCTION

The purpose of the Standard Guide for Credentialing for Access to an Incident or Event Site (hereafter the guide) is to assist in the credentialing of personnel and the associated activities, which allows for access to an incident[2] or event site by State, Tribal, local, private sector, and nongovernmental organizations (NGOs). The credentials allowing scene access should be a verification of identity and (by the authority having jurisdiction [AHJ]) that the appropriate training, experience, and qualifications are in place. This guide does not provide any specifications regarding qualifications or training required for said credentials. However, it is recognized that credentialing is a part of resource management and that a credentialed individual is a specified resource.

1. Scope

1.1 The focus of this guide is on the development of guidelines for credentialing for access. The guide addresses the fundamental terms, criteria, references, definitions, and process model for implementation of credentialing or a credentialing program.

1.2 This guide explains and identifies actions and processes that can provide the foundation for consistent use and interoperability of credentialing for all entities.

1.3 This guide describes the activities involved in creating a credentialing framework, which may include a physical badge; however, it does not define the knowledge, skills, or abilities required to gain access to a site or event. This guide does not address a requirement for a physical badge as a prerequisite for a credential. A badge may be an accepted credential across jurisdictional lines and other credentials may be issues by the AHJ at the scene.

1.4 This guide reinforces the importance of controlling access to a site by individuals with the proper identification, qualification, and authorization, which supports effective management of deployed resources.

1.5 This guide relies on the existing rules, regulations, laws, and policies of the AHJ. Regulations identifying personal and private information as public record may differ from a responder's home jurisdiction.

1.6 This guide utilizes the principles of the Data Management Association Guide to the Data Management Body of Knowledge (DAMA-DMBOK) in order to effectively control data and information assets and does not prescribe the use of technology-based solutions.

1.7 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.8 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *DAMA International:*[3]

The DAMA Guide to the Data Management Body of Knowledge 2009

2.2 *Federal Emergency Management Agency:*

Guideline for the Credentialing of Personnel July 2011

National Response Framework[4] January 2008

NIMS Guide 0002[5] National Credentialing Definition and Criteria, March 27, 2007

[1] This guide is under the jurisdiction of ASTM Committee E54 on Homeland Security Applications and is the direct responsibility of Subcommittee E54.02 on Emergency Preparedness, Training, and Procedures.

Current edition approved June 15, 2021. Published July 2021. Originally approved in 2014. Last previous edition approved in 2014 as E2842 – 14. DOI: 10.1520/E2842-14R21.

[2] As defined in National Incident Management System (NIMS) 2008.

[3] Available from DAMA international, http://www.dama.org/i4a/pages/Index.cfm?pageid=3364.

[4] Available from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

[5] Available from http://www.fema.gov/pdf/emergency/nims/ng_0002.pdf.

NIMS Guideline for the Credentialing of Personnel July 2011

2.3 *Department of Homeland Security:*

NIMS[6] December, 2008

Homeland Security Presidential Directive (HSPD) 12[7] Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

2.4 *NIST Standard:*[8]

FIPS 201 Personal Identification Verification (PIV) of Federal Employees and Contractors and Associated Special Publications (SPs), March 2011

2.5 *NFPA Standard:*[9]

NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, NFPA 2007

NOTE 1—Further information on these subjects can be found in Appendix X1.

3. Terminology

3.1 The following definitions are intended for use in this guide.

3.2 *Definitions:*

3.2.1 *affiliation*—the association of a non-credentialed individual or group of individuals under the supervision of an AHJ-compliant credentialed responder for the purpose of gaining access to accomplish a specific incident or event mission.

3.2.2 *applicant*—an individual applying for a credential.

3.2.3 *attribute*—a qualification, certification, authorization, or privilege of the credential holder.

3.2.4 *Authority Having Jurisdiction (AHJ)*—the organization, office, or individual responsible for enforcing the requirements of a code or standard or approving equipment, materials, an installation, or a procedure. **(NFPA 1600)**

3.2.5 *credential*—a credential is an attestation of the identity, qualification, and authorization of an individual to allow access to an incident or event site.

3.2.6 *credentialing*—the administrative process for validating the qualifications of personnel and assessing their background, for authorization and permitting/granting access to an incident (site or event). **(NIMS Guide 0002)**

3.2.7 *event*—a planned occurrence or large-scale gathering that requires planning, coordination, and support from the emergency management community, such as a National Special Security Event (NSSE) or the Superbowl.

3.2.8 *entity*—a governmental agency or jurisdiction, private or public company, partnership, nonprofit organization, or other organization that has disaster/emergency management and continuity of operations responsibilities. **(NFPA 1600)**

3.2.9 *incident*—an occurrence, natural or man-made, that requires a response to protect life or property. **(NIMS 2008)**

3.2.10 *issuer*—the organization that is issuing a credential to an applicant. Typically, this is an organization for which the applicant is working. **(FIPS 201)**

3.2.11 *National Incident Management System (NIMS)*—a set of principles that provides a systematic, proactive approach guiding government agencies at all levels, the private sector, and NGOs to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment. **(NIMS 2008)**

3.2.12 *Non-Governmental Organization (NGO)*—an entity with an association that is based on the interests of its members, individuals, or institutions. It is not created by government, but it may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations or organizations such as the American Red Cross. **(NIMS 2008, NFR)**

3.2.13 *scene*—the geographical area(s) of an incident with boundaries and access points. There may be multiple levels of a scene that may require multiple access points based upon security, risk, or other factors as defined by the AHJ where different levels of credentialing may be assigned.

3.2.14 *sponsor*—individual or entity endorsing the applicant to receive the credentials.

4. Significance and Use

4.1 There is currently no way to ensure consistency among all entities across the nation for access to an incident or event scene. This guide is intended to enable consistency in credentials with respect to verification of identity, qualifications, and deployment authorization (NIMS 0002).

4.2 This guide is intended to be used by any entity that manages and controls access to an incident scene to facilitate interoperability and ensure consistency.

5. A Framework for the Credentialing of Personnel

5.1 The framework is built upon credentialing principles and elements with an approach that should be established as the initial steps of credentialing activities. The following principles are recommended for consideration:

5.1.1 *Standards Based*—Consistent with applicable national standards or industry-accepted best practices.

5.1.2 *Interoperability*—Ability of systems, personnel, (standards) and equipment to provide and receive functionality, data, information, or services, or combinations thereof, to and from other systems, personnel, and equipment among both public and private agencies, departments, and other organizations in a manner enabling them to operate effectively together (NIMS 2008).

5.1.3 *Trust*—Confidence in the identity and qualifications of the individual, and confidence in the manner in which the credentials are validated at the scene.

[6] Available from http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

[7] Available from U.S. Government Printing Office Superintendent of Documents, 732 N. Capitol St., NW, Mail Stop: SDE, Washington, DC 20401, http://www.access.gpo.gov.

[8] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

[9] Available from National Fire Protection Association (NFPA), 1 Batterymarch Park, Quincy, MA 02169-7471, http://www.nfpa.org/assets/files/dpf/nfpa1600.pdf.

5.1.4 *Physical and Cyber Security*—Use of best practices to protect the physical credential and associated data. Refer to the Data Security Management section of Appendix X3 for more information.

5.1.5 *Privacy*—To protect an individual's private information in accordance with applicable laws; for example, name, social security number, biometric records, medical records, or tribal enrollment.

5.1.6 *Transparency*—Policies are implemented in an open and understandable manner.

5.1.7 *Sustainability and Portability*—Capacity to maintain credentialing activities and to remain effective when the AHJ or the overall authority, or both, changes.

5.2 *Credentialing Program Elements*—The following credentialing program elements are recommended building blocks for a credentialing framework: planning, funding, implementation, agreements, information management, training and exercises, and audit process. For more information, refer to Appendix X4 – Sample Credentialing Plan Template.

5.2.1 *Planning*—Planning should consider the jurisdiction's strategy for credentialing as well as development of plans to address goals, objectives, and business rules. Planning should also establish roles and responsibilities and address the implementation process and supporting procedures.

5.2.2 *Business Rules*—The AHJ should detail how credentials will be granted, including to whom and through what authorization process. Rules must include a provision and plan to ensure private information is protected through the adherence to privacy laws and policies, information management, and protection processes. Business rules should include a process for verification of a person's identification, verification of attributes, and deployment authorization. Business rules should also be in place for access permissions (from least secure to most secure) at incident scenes requiring varying security perimeters. Additionally, rules should include a process for appeal and reciprocity across jurisdictional boundaries.

5.2.3 *Credential Elements*—Credentials can be anything used to identify that a person's identity, qualifications, and authorization have been validated, for example badges, arm bands, vest, clothing, index cards, or any combination of mechanisms. The following is a list of elements that may be considered to develop to verify identification, qualification, and authorization information:

(1) Photograph,
(2) Name (Last, First, Middle Initial),
(3) Organization Represented,
(4) Employee Affiliation,
(5) Organizational Affiliation,
(6) Expiration Date,
(7) Area for Circuit Chip/Contact Chip/Smart Chip,
(8) Date Issued,
(9) Header (such as State, local, Tribal, private sector, or NGO),
(10) Footer (such as Federal Emergency Response Official (FERO) Designation),
(11) Agency Seal Watermark,
(12) Agency Card Serial Number,
(13) Issuer Identification,
(14) Qualification Information,
(15) Authorization Information (to deploy),
(16) Signature,
(17) Agency-specific Text Area,
(18) Rank,
(19) PDF Bar Code,
(20) Color Coding for Employee Affiliation,
(21) Photo Border for Employee Affiliation,
(22) Agency-specific Data,
(23) Magnetic Strip,
(24) Return to "If Lost" Language,
(25) Physical Characteristics of Cardholder,
(26) Additional Language for Emergency Responder Officials,
(27) Standard Section 499, Title 18 Language,
(28) Linear 3 of 9 Bar Code, and
(29) Agency-specific Text.

Depending upon the credentialing solution based on the entity's credentialing plan, there may be specific requirements for data or placement. Refer to Appendix X2 for example credentials.

5.2.4 *Distribution*—This should include ways of maintaining control of credentials while distributing to the appropriate parties or responders. This process shall also account for lost, stolen, or revoked credentials, or combinations thereof.

5.2.5 *Timelines/Schedules*—These elements should detail any phased approach for implementation or maintenance of the credentialing program.

5.2.6 *Needs Assessment*—The needs assessment identifies and validates the target audience and requirements for the credentialing plan and process, including identification of those with a potential need for access, numbers and types of individuals in a given skill area, and the status of extant credentials in that area.

5.2.7 *Plans and Procedures*—The credentialing plan should include:

5.2.7.1 *Purpose*—Describe the reasoning for the development of a credentialing plan.

5.2.7.2 *Scope*—Applicability of the plan, the items for inclusion, and the intended audience.

5.2.7.3 *Definitions*—Specific definitions for key words used in the plan.

5.2.7.4 *Authorities*—Applicable legislation, regulations, directives, or policies, or combinations thereof, to create and implement the credentialing plan. For more detailed information about data protection, see Appendix X3.

5.2.7.5 *Governance*—Planning, supervision, and control of the credentialing process.

5.2.7.6 *Credentialing Principles*—State the over-arching guidance for the approach of the AHJ (see above).

5.2.7.7 *Approach*—A high-level description of how the entity structures its plan to credential different types and numbers of individuals, for example, emergency responders, other government agencies, elected officials, tribal leaders, media, and volunteers. This approach should be scalable to rapidly expand or contract to meet incident or event requirements.