Designation: E2842 − 14

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 and health practices and determine the applicability of regulatory limitations prior to use.*

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.

NIMS Guideline for the Credentialing of Personnel July 2011.

2.3 *Department of Homeland Security:*

NIMS[6] December, 2008

Homeland Security Presidential Directive (HSPD)

[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 March 1, 2014. Published March 2014. DOI: 10.1520/E2842-14.

[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.

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

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.

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.

[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..

5.1.5 *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
(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.

5.2.7.8 *Implementation Process*—The activities included in the credentialing implementation process.

5.2.7.9 *Documentation*—Records kept by an entity to ensure the validity of an individual's credential.

5.2.8 *Pilot Program*—Prior to the implementation of credentialing activities, a pilot project should be conducted in order to test and evaluate an entity's activities. A pilot project has the added complexity of a requirements assessment, strategy development, technology evaluation selection, and initial implementation cycle that subsequent incremental projects may not have.

5.3 *Funding*—Funding for initiation and sustaining of a viable credentialing program should be identified prior to initiating a program. A line item in the jurisdiction's budget should be created and approved that supports the strategy, goals, objectives, and implementation of the program. Funding for current and future maintenance and sustainment activities should be included. The budget should address pilot or demonstration project costs if these initiatives would promote program support and sustainment.

5.3.1 *Initial Funding*—Funding should be identified to include startup costs associated with implementing a new credentialing program. Costs covering complete assessment of the credentialing activities and specifics pertaining to roll-out should be considered. The credentialing solution does not have to be capital intensive and does not have to be based on technology; it can be as simple as providing wristbands to those arriving on the scene.

5.3.2 *Sustained Funding Source*—As credentialing activities may be capital intensive, a sustained funding source should be locked in as part of the planning process to ensure that the activities can be sustained. The funding should be identified for any pilot, phases, or iterations, and through at least two additional cycles following the initial introduction of the credentials. The program should also include a cost accounting and tracking mechanism for all funding.

5.4 *Implementation*—Should provide targeted instructions for ensuring that the plan and program are successfully integrated into operations. The implementation plan may be divided into phases, sections, or subsets to allow for an incremental implementation of parts of the plan. The plan should include the process for:

5.4.1 *Request*—This activity applies to the initiation of a request by an applicant or sponsor for the issuance of a credential to the applicant and the validation of this request by the sponsor.

5.4.2 *Enrollment and Registration*—The goal of this activity is to verify that the claimed identity of the applicant and the entire set of identity source documents presented at the time of registration are valid. Background verification according to the entity's laws, policies, or processes should be conducted as a part of this process.

5.4.3 *Issuance*—This activity deals with the personalization of the credential and the issuance of the credential to the intended applicant. Credentials should be issued through a managed, coordinated system detailed in the implementation plan. Standardized requirements for issuers should be developed and promulgated to all authorized issuers. The process and logistical and information support requirements for the issuance of credentials should be detailed for all issuers. The issuance process should delineate the required personnel and their separate and distinct roles, which may include:

5.4.3.1 *Applicant*—Individual applying for the credential.

5.4.3.2 *Sponsor*—Individual or entity endorsing the applicant to receive credential.

5.4.3.3 *Enrollment Official*—Individual enrolling the applicant's information into the issuance system. This position should not be held by the same person as the Issuance Officer/Entity.

5.4.3.4 *ID Validator/Adjudicator*—Individual or board verifying all information and resolving any issues/conflicts related to the applicant's information.

5.4.3.5 *Issuance Officer/Entity*—Individual or body physically issuing the credential to the sponsored and approved applicant. This position should not be held by the same person as the Enrollment Officer.

5.4.4 *Usage*—During this activity, the credential is used to authenticate the credential holder for access to an incident scene or other resource. Access authorization decisions are made after successful credential holder identification and authentication.

5.4.4.1 Different levels of access permissions/perimeters may be assigned or identified within an incident scene as determined by the incident command.

5.4.4.2 In the event of a lost, compromised, or falsified credential, termination or revocation of the credential may be required.

5.4.5 *Maintenance*—This activity delineates the currency process to include renewal, reissuance, or update of the credential. Refer to Data Security Management in Appendix X3 for more information.

5.4.6 *Termination/Revocation*—The termination/revocation process is used to permanently destroy or invalidate the credential and the data and keys needed for authentication so as to prevent any future use of the information for authentication. Ensure terminations/revocations are implemented on a timely basis to minimize any negative impacts to the scene and the AHJ. Policies and procedures for credentialing activities can include detailed steps on how to terminate or revoke a credential in the event of lost, compromised, or falsified credentials. Refer to Data Security Management in Appendix X4 for more information.

5.5 *Agreements*—Agreements should be established in advance of implementation of credentialing activities for access to an incident or event. Consider all partners that may require access to the incident or event site. Begin with a list of those partners typically involved in joint training and exercising events and then identify those that may be required for specific situations, hazards, or events. In developing agreements, share information regarding the credentialing program and processes with potential partners or stakeholders, or both.

5.6 *Information Management*—Information as it relates to credentialing comes in many forms of data, such as personnel qualifications, identification, and deployment authorization documents. The management of personnel data requires a method for acquiring, validating, storing, protecting, and processing information, which can then be used to grant authorization for access to an incident scene or event site. Data management comprises all the disciplines or communities of practice, or both, related to managing information as a valuable resource as applicable to credentialing activities. The principles of data management (sometimes used interchangeably with information management), listed in the numbered list below, are relevant to manual as well as automated systems. Both entities with large, sophisticated, automated credentialing systems as well as entities with small, manual, procedurally-based credentialing systems should address data management. The following ten areas should be addressed as part of an information or data management process:

(1) Data Governance
(2) Data Architecture Management
(3) Data Development
(4) Data Operations Management
(5) Data Security Management
(6) Reference and Master Data Management
(7) Data Warehousing and Business Intelligence Management
(8) Document and Content Management
(9) Meta-data Management
(10) Data Quality Management

Additional information on the ten elements of data management can be found in Appendix X3. The information in Appendix X3 is technical in nature and is intended for use primarily by technical or support personnel in the development of credentialing data, processes and systems in accordance with this guide.

5.7 *Training and Exercises*—The credentialing plan should include the baseline training requirements for each key person engaged in the credentialing activities, including distributing, utilizing, and recognizing valid credentials, and terminating/revoking credentials. Personnel should be regularly trained on their respective credentialing activities. Exercises should be routinely conducted on the credentialing plan, policies, and procedures with improvements being made on exercise findings and evaluation.

5.8 *Audit Process*—The credentialing plan should include an audit process from an external source if possible.

5.9 *Contingency*—There should be some type of backup plan and procedures in place should there be any issue with interoperability or technology to credential onsite during disaster or event operations. The contingency should be scalable to rapidly expand or contract to meet incident or event requirements.

6. Access Control of Affiliates

6.1 Access Control is the process by which personnel and resources are granted entry into an established perimeter of an incident or event site, typically validated with an AHJ-compliant credential. Varying points of entry may be established based on the type of severity of the event. Plans should involve a phased approach for re-entry of displaced citizens and critical resources.

6.2 Affiliation is the process through which non-credentialed individuals or groups of individuals gain access to a controlled area under the supervision of AHJ-compliant credentialed personnel. Affiliated personnel may require specific, targeted access to an incident or event site to accomplish a stated mission. This process is applied when the volume of required credentials exceeds the capacity and efficiency of the credentialing system to issue individual credentials in a timely manner.

6.3 The AHJ-compliant sponsor should have documentation that verifies the affiliation of individuals. Documentation includes a list of individuals associated with an AHJ-compliant credential for verification of affiliation and should accompany the AHJ request for personnel and equipment needed to verify deployment authorization.

7. Keywords

7.1 attributes; credentials; emergency management; emergency site access; homeland security; identification

APPENDIXES

(Nonmandatory Information)

X1. CREDENTIALING REFERENCE/RESOURCE LIST

X1.1 *Governor's Office of Administrative/Office for Information Technology, Identity Protection and Access Management (IPAM) Architectural Standard – Identity Management Services*, Commonwealth of Pennsylvania, June 22, 2006. Available from URL: www.portal.state.pa.us.

X1.2 *FIPS Publication (FIPS PUB 201-1); PIV of Federal Employees and Contractors*, Department of Commerce, March 2006. Available from URL: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

X1.3 *Memorandum (and Attachment) on the DoD Acceptance and Use of Personal Identity Verification – Interoperable (PIV-I) Credentials*, Department of Defense, October 5, 2010.

X1.4 *Best Practices: Incident Site Security, Perimeter Security, Credentialing*, DHS. Available from URL: http://www.llis.gov. Access to LLIS will require user to follow prompts to register for LLIS.

X1.5 *HSPD – 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, DHS, August 27, 2004.

X1.6 *Moving Towards Credentialing Interoperability: Case Studies at the State, Local, and Regional Levels*, DHS, July 2010. Available from URL: http://www.dhs.gov/xlibrary/assets/st-credentialing-interoperability.pdf.

X1.7 *National Infrastructure Protection Plan*, DHS 2009.

Available from URL: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

X1.8 *National Response Framework*, DHS, January 2008. Available from URL: http://www.fema.gov/emergency/nrf/.

X1.9 *Credentialing Project Overview*, Eastern Colorado Incident Management Team, 2009.

X1.10 *Continued Implementation of HSPD 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, Executive Office of the President, February 3, 2011.

X1.11 *Implementation of HSPD 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, Executive Office of the President, August 5, 2005.

X1.12 *Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guide*, Federal Chief Information Officers Council and the Federal Enterprise Architecture, November 10, 2009.

X1.13 *Federal Chief Information Officer Council, Personal Identity Verification Interoperability for Non-Federal Issuer*, Federal Chief Information Officer Council, May 2009. Available from URL: http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf.

X1.14 Lessons Learned Information Sharing, FEMA. Available from URL: https://www.llis.dhs.gov/index.do.

X1.15 *National Emergency Responder Credentialing System*, FEMA National Integration Center, October 24, 2005.

X1.16 *Spring Forwards Federal and Mutual Aid Emergency Response Official Electronic Credentialing & Validation Interoperability Demonstration: After Action Report*, FEMA, March 12, 2010. Available from URL: http://www.llis.dhs.gov.

X1.17 *National Continuity Policy Implementation Plan*, Homeland Security Council, August 2007. Available from URL: http://www.fema.gov/pdf/about/org/ncp/ncpip.pdf.

X1.18 Information Technology – Automatic Identification and Data Capture Techniques: PDF417 Bar Code Symbology Specifications (ISO/IEC 15438:2006), International Organization for Standardization, 2006. Available from URL: http://www.iso.org/iso/iso_catalogue_tc/catalogue_detail.htm?csnumber=43816.

X1.19 *Credentialing Program and Operating Guidelines and Procedures*, North Central Region (Denver, Colorado), Version 1.0 Final. August 2010.

X1.20 *NFPA 1561, Standard on Emergency Services Incident Management System*, NFPA, 2008. Available from URL: http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1561.

X1.21 *NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs*, NFPA, 2007. Available from URL: http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf.

X1.22 National Institute of Standards and Technology. *NIST Special Publication 800-116. A Recommendation for the Use of PIV Credentials in Physical Control Systems (PACS).* November 2008.

X1.23 *FIPS PIV of Federal Employees and Contractors and Associated Special Publications (SPs)*, National Institute of Standards and Technology, March 2011.

X1.24 *Federal Information Processing Standards Publication, 55-3, Codes for Named Populated Places, Primary County Divisions, and Other Locational Entities of the United States, Puerto Rico, and Outlying Areas*, National Institute for Standards and Technology, December 28, 1994. Available from URL: http://www.itl.nist.gov/fipspubs/fip55-3.htm.

X1.25 *Memorandum for Heads of Departments and Agencies Re: Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12*, Office of Management and Budget, July 31, 2008. URL: http://www.hss.doe.gov/deppersonnelsec/guidance/Final_Credentialing_Standards_for_Issuing_PIV_Cards.pdf.

X1.26 *Memorandum M-11-11 (OMB M-11-11), Continued Implementation of Homeland Security Presidential Directive (HSPD)-12*, Executive Office of the President, February 3, 2011. Available from URL: www.whitehouse.gov/sites/default/files/omb/memorada/2011/m11-11.pdf.

X1.27 *Colorado State First Responder Authentication Credential Standards: Best Practice Standard*, State of Colorado, Governor's Office of Information Technology, April 10, 2010.

X1.28 *The State of Colorado First Responder Authentication Credential (COFRAC); Business Process for Statewide Implementation of Standards and Credentials*, State of Colorado, DRAFT.

X1.29 *Standard Operating Procedure: Statewide Credentialing/Access Program*, State of Louisiana. Available from URL: http://www.gohsep.la.gov/plans/lscap.pdf.

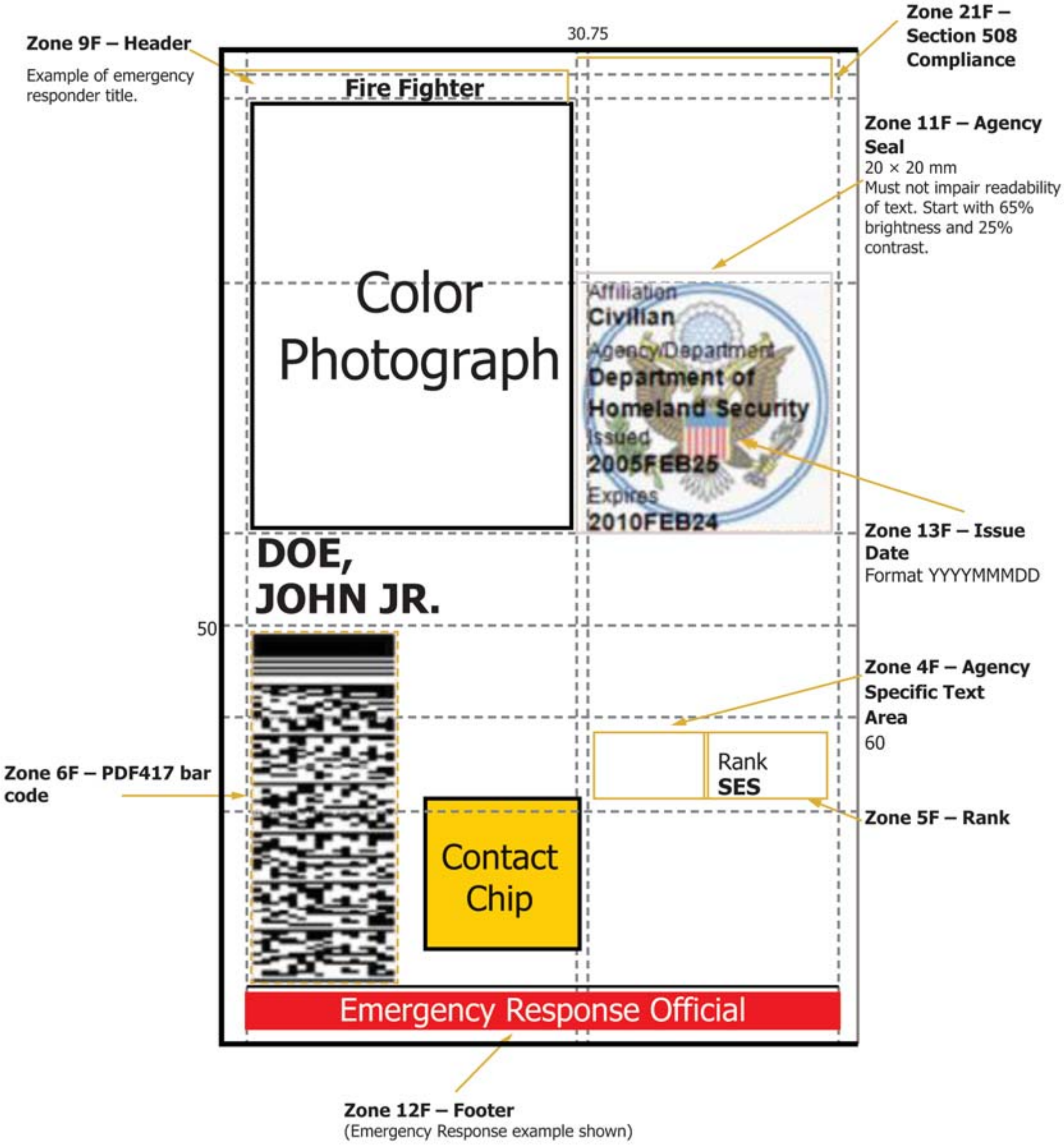
X1.30 *West Virginia Region III Credentialing Pilot*, West Virginia Division of Homeland Security and Emergency Management, November 18, 2009. Available from URL: www.llis.dhs.gov.

X1.31 *Presidential Policy Directive: PPD-8 National Preparedness*, The White House, March 30, 2011.

X2. CREDENTIAL COMPONENTS

X2.1 The graphics below were taken from the *Federal Information Processing Standards Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors*, DRAFT March 2011. (See Figs. X2.1-X2.5.)

X2.2 Below are examples of credentials in addition to the traditional badge often used by the Federal government. (See Figs. X2.6-X2.13.)



Zone 9F – Header
Example of emergency responder title.
30.75
Zone 21F – Section 508 Compliance
Fire Fighter
Color Photograph
Zone 11F – Agency Seal
20 × 20 mm
Must not impair readability of text. Start with 65% brightness and 25% contrast.
Affiliation
Civilian
Agency/Department
Department of Homeland Security
Issued
2005FEB25
Expires
2010FEB24
Zone 13F – Issue Date
Format YYYYMMMDD
DOE, JOHN JR.
50
Zone 4F – Agency Specific Text Area
60
Rank
SES
Zone 5F – Rank
Zone 6F – PDF417 bar code
Contact Chip
Emergency Response Official
Zone 12F – Footer
(Emergency Response example shown)

FIG. X2.1 Example 1

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5 pt normal weight for tags and 6 pt bold for data.

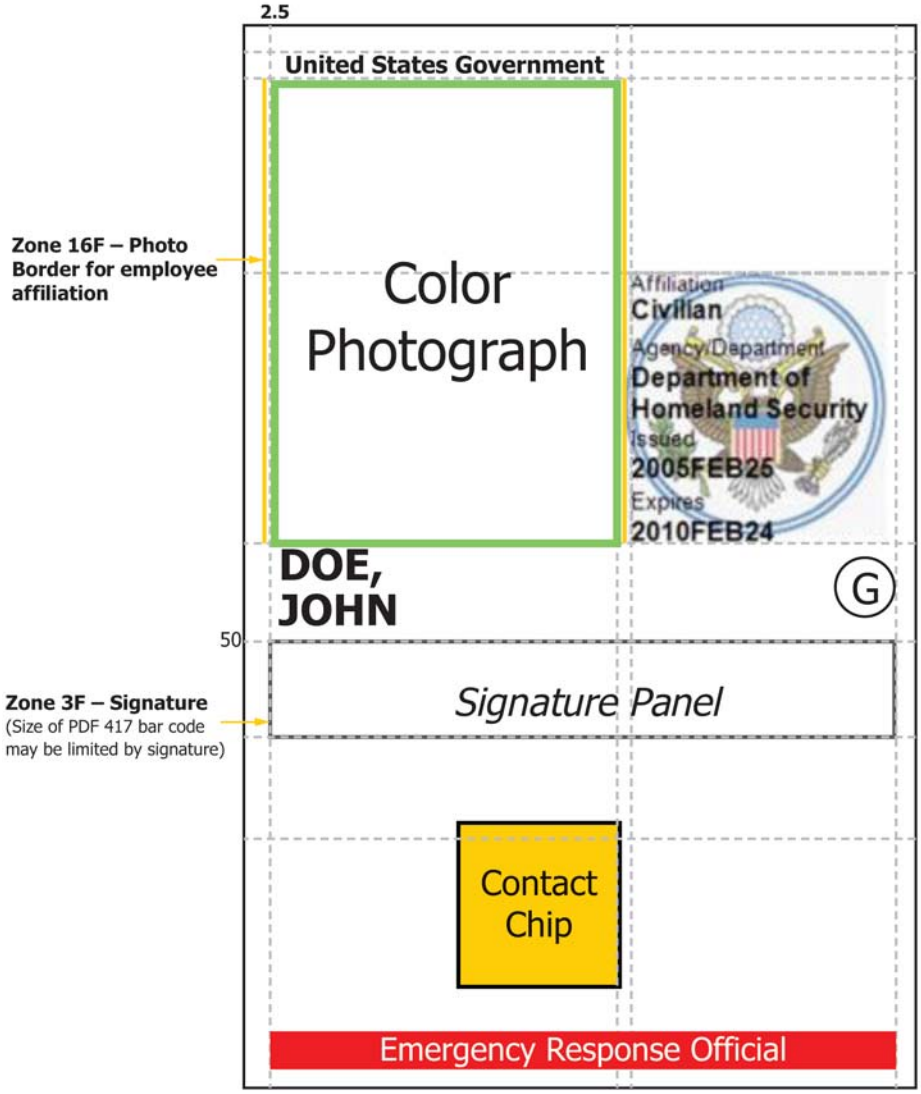


FIG. X2.2 Example 2

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to printed using the Arial font.
Unless otherwise specified, the font size should be 5 pt normal weight for tags and 6 pt bold for data.

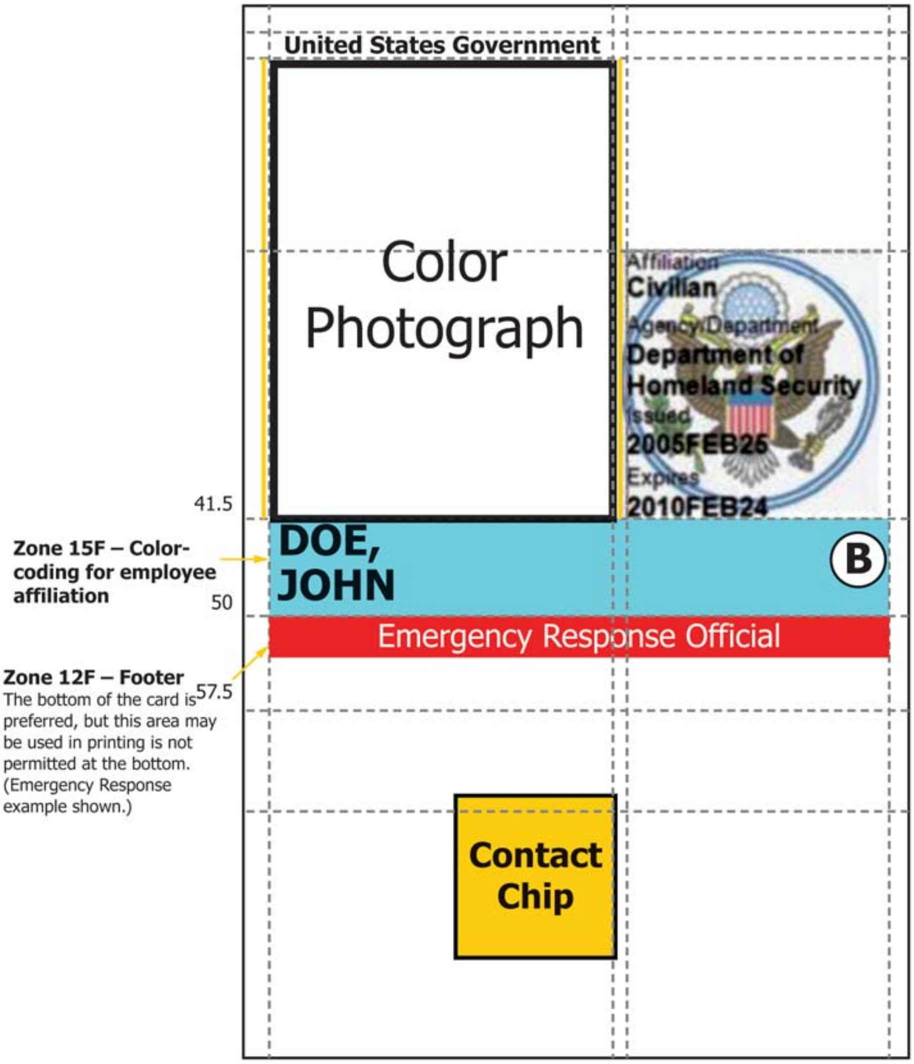

United States Government
Color Photograph
Affiliation
Civilian
Agency/Department
Department of Homeland Security
Issued
2005FEB25
Expires
2010FEB24
41.5
Zone 15F – Color-coding for employee affiliation
DOE, JOHN
B
50
Emergency Response Official
Zone 12F – Footer
The bottom of the card is preferred, but this area may be used in printing is not permitted at the bottom. (Emergency Response example shown.)
57.5
Contact Chip

FIG. X2.3 Example 3

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5 pt normal weight for tags and 6 pt bold for data.

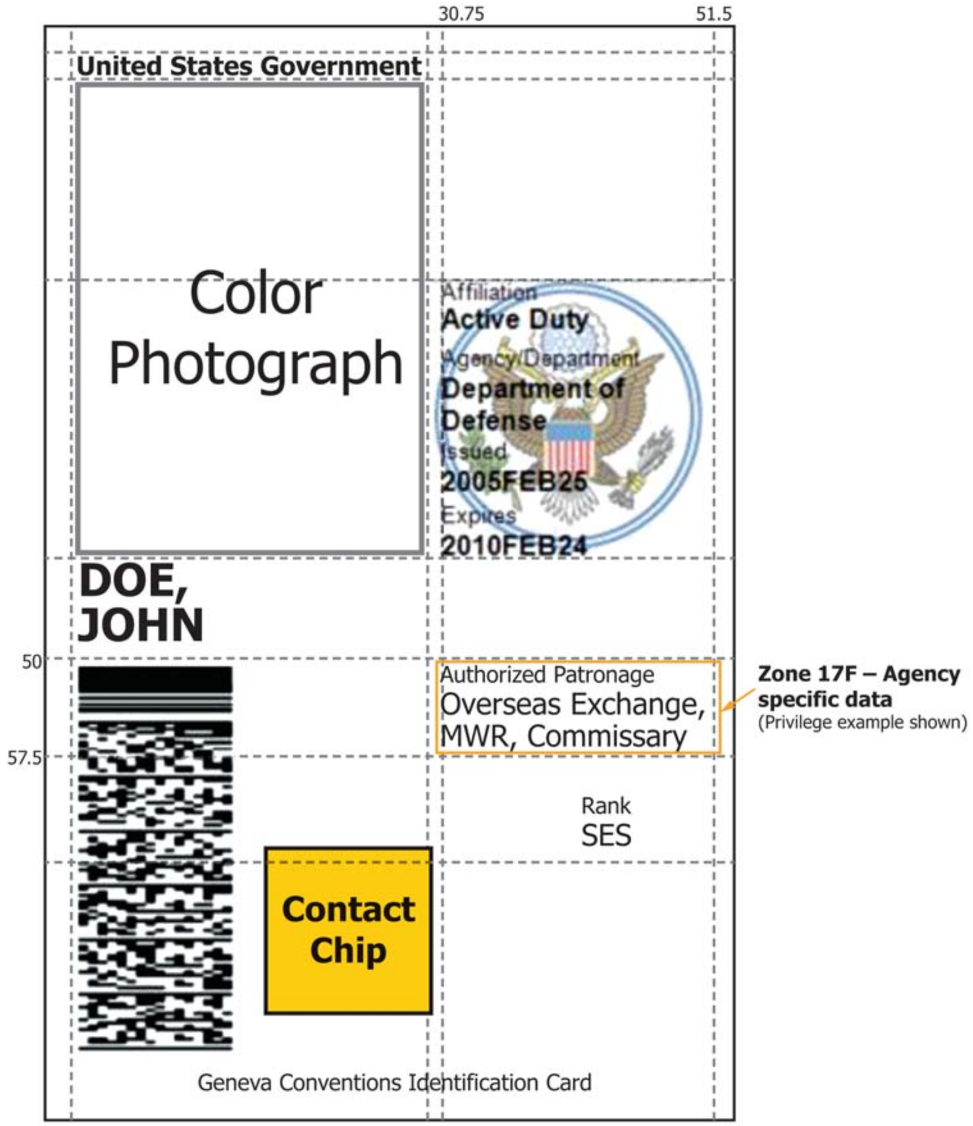
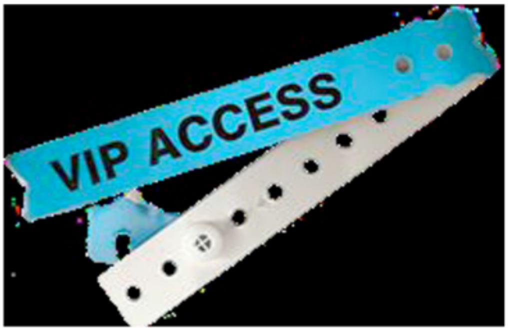
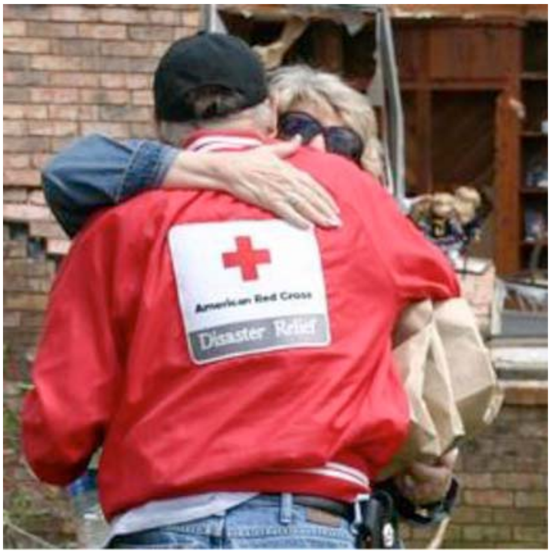


FIG. X2.4 Example 4



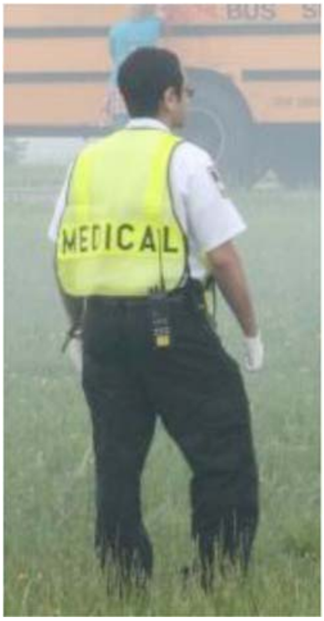
NOTE 1—Example of a wristband, which can give the wearer access to restricted areas. (This image was taken from: http://photobusinessforum.blogspot.com/2007_09_16_archive.html.)

FIG. X2.5 Example 5



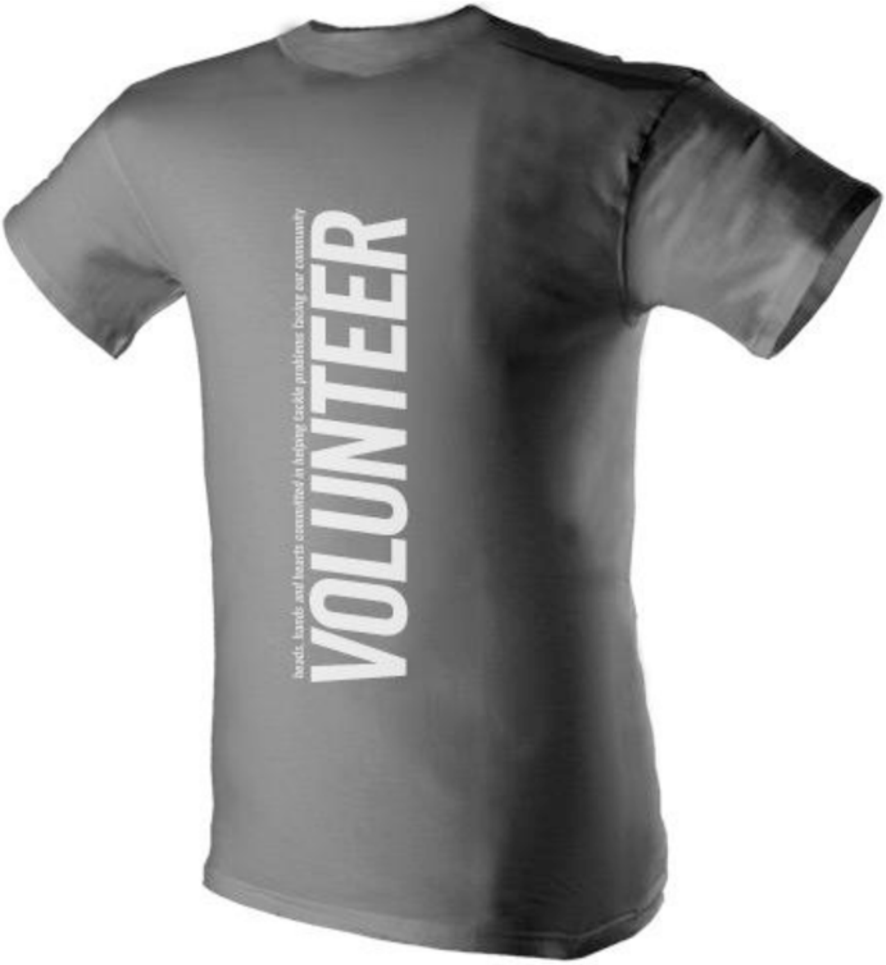
NOTE 1—Different types of apparel can signify the affiliation of the wearer, such as with the American Red Cross jacket this Relief Worker is wearing. (This image was taken from: http://www.redcross.org/ok/tulsa.)

FIG. X2.6 Example 6



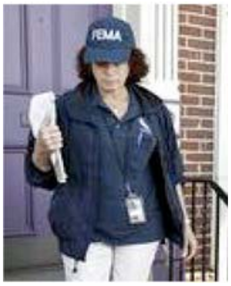
NOTE 1—A simple vest can signify the role of the wearer. (This image was taken from http://news.psu.edu/photo/259140/2013/02/11/airport-disaster-drill-7.)

FIG. X2.7 Example 7


VOLUNTEER
heads, hands and hearts committed to helping tackle problems facing our community

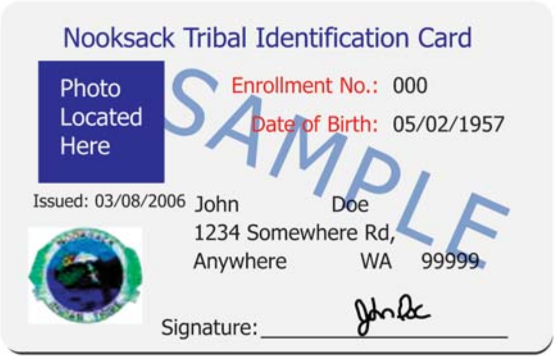
NOTE 1—A t-shirt can signify the role of the wearer, such as this t-shirt worn by United Way volunteers. (This image was taken from http://www.unitedwaystore.com/product/Volunteer_T-Shirt/tshirts_apparel.)

FIG. X2.8 Example 8



NOTE 1—A hat is a good example of an easy way to identify the role or affiliation of the wearer. (This image was taken from http://www.pennlive.com/midstate/index.ssf/2011/10/flood_affected_residents_vent.html.)

FIG. X2.9 Example 9



Nooksack Tribal Identification Card

Photo
Located
Here

Enrollment No.: 000

Date of Birth: 05/02/1957

SAMPLE

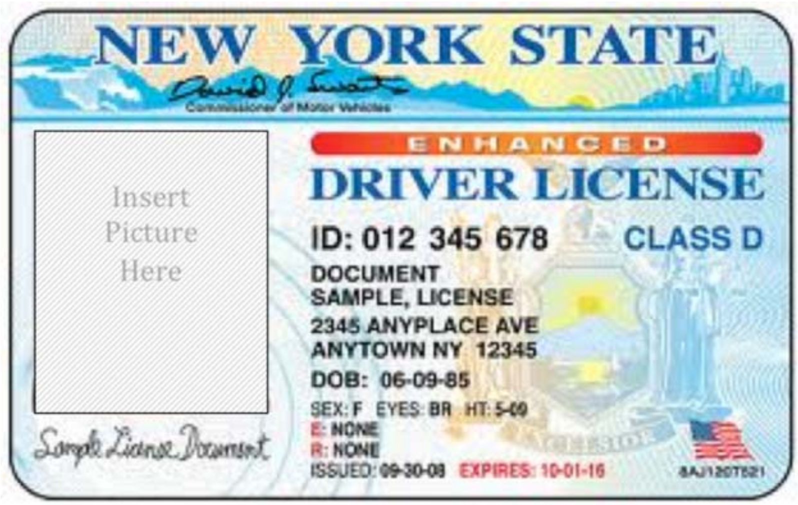
Issued: 03/08/2006

John Doe
1234 Somewhere Rd,
Anywhere WA 99999

Signature:

NOTE 1—Native American Tribes have unique identification cards that can serve as an alternative credential, such as the one above. (This image was taken from http://liq.wa.gov/rules/tribal-ID-cards)

FIG. X2.10 Example 10



NEW YORK STATE

Commissioner of Motor Vehicles

ENHANCED

DRIVER LICENSE

Insert
Picture
Here

ID: 012 345 678 CLASS D

DOCUMENT
SAMPLE, LICENSE
2345 ANYPLACE AVE
ANYTOWN NY 12345

DOB: 06-09-85

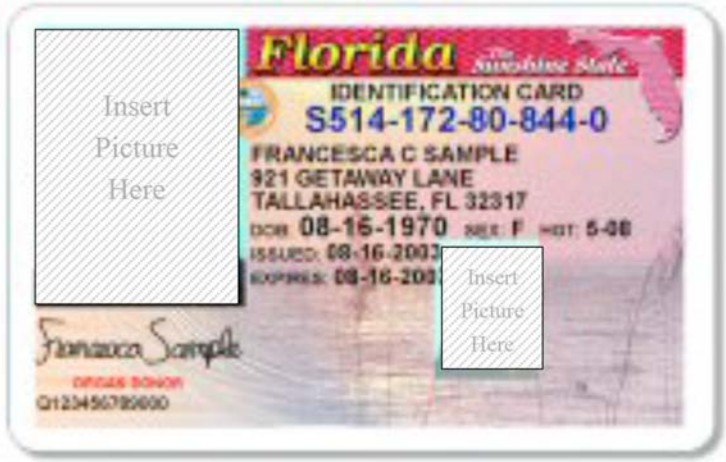
SEX: F EYES: BR HT: 5-09
E: NONE
R: NONE
ISSUED: 09-30-08 EXPIRES: 10-01-16

8AJ1207521

Sample License Document

NOTE 1—A driver's license is one of the most common alternate types of credentials. (This image was taken from http://cityroom.blogs.nytimes.com/2008/09/17/a-new-license-for-more-than-just-driving/)

FIG. X2.11 Example 11



Florida The Sunshine State

IDENTIFICATION CARD

S514-172-80-844-0

FRANCESCA C SAMPLE
921 GETAWAY LANE
TALLAHASSEE, FL 32317

DOB 08-16-1970 SEX F HGT 5-08

ISSUED: 08-16-2003

EXPIRES: 08-16-200

Insert Picture Here

Insert Picture Here

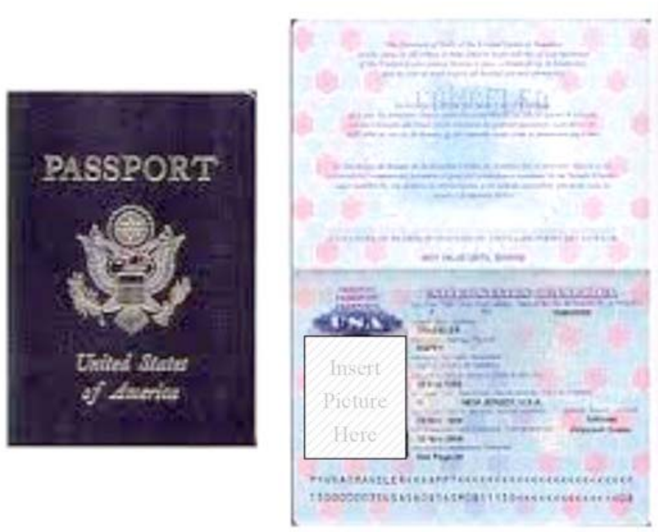
Francesca Sample

ORGAN DONOR

Q123456789000

NOTE 1—An identification card is similar to a driver's license in that it contains identification information, which makes it a good example of an alternative credential. (This image was taken from http://www.flhsmv.gov/safetytips/IDSafety.htm)

FIG. X2.12 Example 12



NOTE 1—A passport is another one of the most common alternate types of credentials. (This image was taken from http://pd.scisdragons.net/pvalenza/2011/09/22/56756/sample-usa-passport/)

FIG. X2.13 Example 13

X3. DATA MANAGEMENT OVERVIEW

INTRODUCTION

The management of personnel data requires a method for acquiring, validating, storing, protecting, and processing information, which can then be used to grant authorization for access to an incident or event site. The principles of data management, included below, should be considered and addressed as part of a data or information management process as identified in the DAMA DM-BOK Guide (reference 5.6 of this guide).

The information in this Appendix is technical in nature and is intended for use primarily by technical or support personnel, or both, in the development of credentialing data, processes, and systems in accordance with this guide. (See *The DAMA Guide to the Data Management Body of Knowledge*, DAMA International, 2004 and Fig. X3.1.)

X3.1 Data Governance

X3.1.1 The exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets. Data Governance is high-level planning and control over data management.

X3.2 Data Architecture Management

X3.2.1 Defining the data needs of the enterprise (for example, organization wide) and designing the master blueprints to meet those needs. This functioning includes the development and maintenance of enterprise data architecture

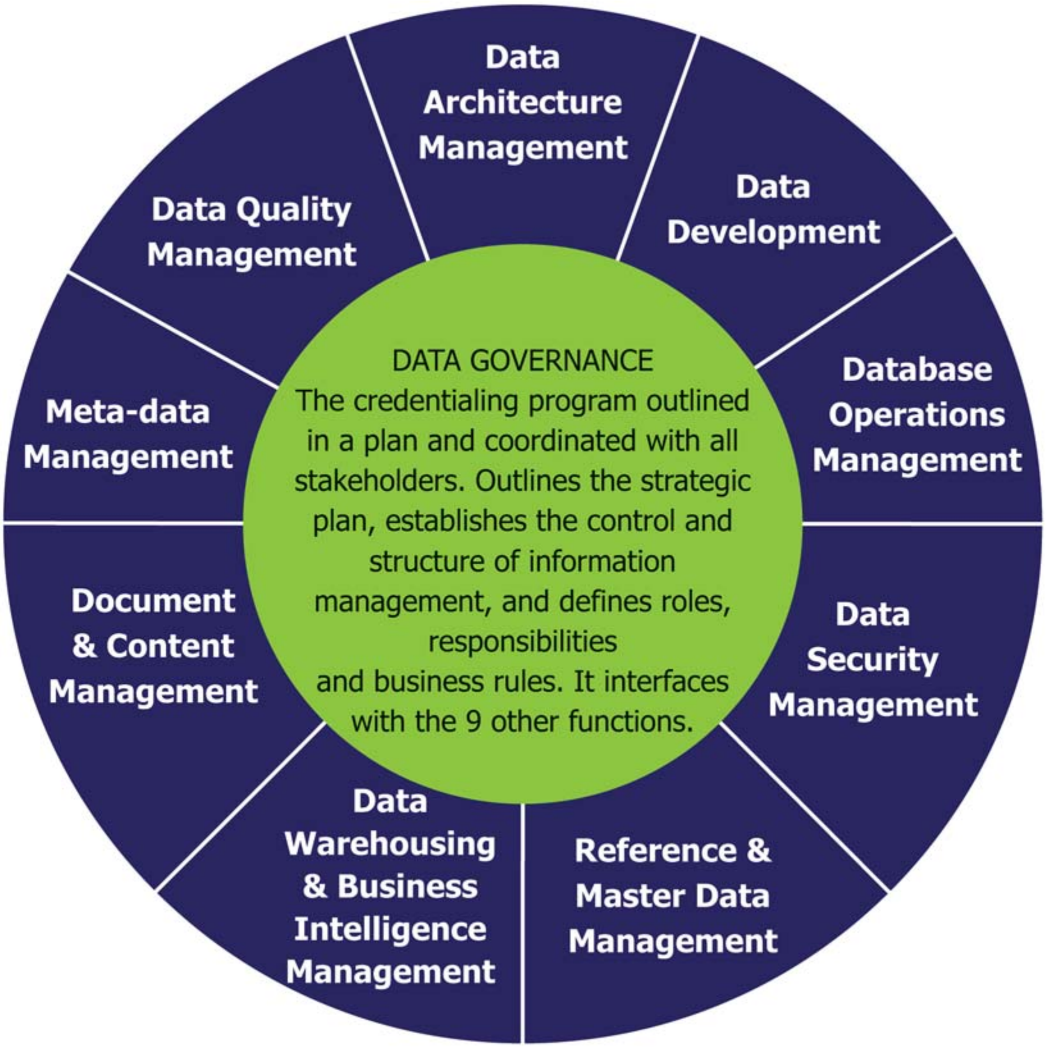

Data Architecture Management
Data Development
Database Operations Management
Data Security Management
Reference & Master Data Management
Data Warehousing & Business Intelligence Management
Document & Content Management
Meta-data Management
Data Quality Management
DATA GOVERNANCE
The credentialing program outlined in a plan and coordinated with all stakeholders. Outlines the strategic plan, establishes the control and structure of information management, and defines roles, responsibilities and business rules. It interfaces with the 9 other functions.

FIG. X3.1 Data Management Elements

within the context of all enterprise architecture and its connection with the application system solutions and projects that implement enterprise architecture.

X3.3 Data Development

X3.3.1 Designing, implementing, and maintaining solutions to meet the data needs of the enterprise. The data-focused activities within the system development lifecycle (SDLC) including data modeling, data requirements analysis and design, implementation, and maintenance of data-related solution components.

X3.4 Data Operations Management

X3.4.1 Planning, control, and support for structured data assets across the data lifecycle, from creation and acquisition through archiving and purging.

X3.5 Data Security Management

X3.5.1 Planning, development, and execution of security policies and procedures to provide proper authentication, authorization, access, and auditing of data and information.

X3.6 Reference and Master Data Management

X3.6.1 Planning, implementation, and control activities to ensure consistency with a "golden version" of contextual data values.

X3.7 Data Warehousing and Business Intelligence Management

X3.7.1 Planning, implementation, and control processes to provide decision support data and support for knowledge workers engaged in reporting, query, and analysis.

X3.8 Document and Content Management

X3.8.1 Planning, implementation, and control activities to store, protect, and access data found within electronic files and physical records (including text, graphics, images, audio, and video).

X3.9 Meta-Data Management

X3.9.1 Planning, implementation, and control activities to enable easy access to high quality, integrated meta-data.

X3.10 Data Quality Management

X3.10.1 Planning, implementation, and control activities that apply quality management techniques to measure, assess, improve, and ensure the fitness of data for use.

X4. SAMPLE CREDENTIALING PLAN TEMPLATE

INTRODUCTION

The following outline should be used as a template to begin the process of establishing a credentialing plan for access to an incident or event site. These components should be considered suggestions and should be used in whole or in part as they pertain to your entity's needs.

X4.1 *Abstract*—Summation of the plan and the program.

X4.2 *Plan Overview*:

X4.2.1 *Purpose*—Purpose for the plan or program, or both. This will include the Approach, a high-level description of how the entity structured its plan to credential different types and numbers of individuals.

X4.2.2 *Scope*—Entities or situations, or both, for which the plan or program, or both, is intended.

X4.2.3 *Definitions*—Specific definitions for key words used in the plan (may include roles or positions).

X4.2.4 *Authorities*—Applicable legislation, regulations, directives, or policies, or combinations thereof, to create and implement the plan.

X4.2.5 *Governance*—Planning, supervision, and control of the credentialing process.

X4.2.6 *Program Principles*—Review the over-arching principles that the program encompasses.

X4.2.6.1 *Standard*—The accepted standard for which the program follows or is in line with.

X4.2.6.2 *Interoperability Picture*—The standards or infrastructure, or both, that facilitates interoperability among entities participating in the program.

X4.2.6.3 *Security and Privacy*—Overview of applicable laws and information privacy practices.

X4.2.6.4 *Sustainability/Maintenance*—By whom, how, and when the plan and program are updated and maintained.

X4.3 *Planning*—Pre-operational implementation of the program.

X4.3.1 *Goals and Objectives*—The mission and actions associated with achieving the mission of the plan or program, or both. This will include the Timeline/Schedule and a review of the implementation schedule.

X4.3.2 *Business Rules*—The over-arching process for how credentials are issued.

X4.3.3 *Requirements*—How an agency transitions or participates in the program.

X4.3.4 *Agency Roles and Responsibilities*—Roles and responsibilities of entities participating in the plan or program, or both.

X4.3.5 *Credential Elements*—Definition of credential type and elements.

X4.3.6 *Data Management*—Review of the ten principles of data management and how they are being used to support the implementation of the plan or program, or both.

X4.3.7 *System Components*—Outline of the components of the program to include equipment, personnel, activation information, etc. One of the components, IT Infrastructure, is a description of the IT backbone for the program, including who can access it and how.

X4.3.8 *Physical and Cyber Security Protocols*—Description of the protocols necessary for the security of physical credentials and personal identification information.

X4.4 *Implementation*—Targeted instructions for ensuring that the plan or program, or both, are successfully integrated into operations including the process for the issuance of credentials.

(a) Request
(b) Enrollment/Registration
(c) Issuance
(d) Usage
(e) Maintenance
(f) Termination/Revocation
(g) Agreements
(h) Information Management
(i) Training and Exercise
(j) Audit Process
(k) Contingency
(l) Policy for Access Control of Affiliates

X4.5 Suggested supplemental sections or appendixes:

(1) Documentation (Forms),
(2) Mutual Aid Agreements, etc.,
(3) Vendor information or documentation, or both,
(4) Process flow chart,
(5) Points of Contact for participating agencies, signatories, etc.,
(6) Program training and exercise plan and schedule,
(7) Pilot program after action review,
(8) Funding information including budget and funding source for sustainment,
(9) Definitions/Key Terms, and
(10) Acronym List.

ASTM International takes no position respecting the validity of any patent rights asserted in connection with any item mentioned in this standard. Users of this standard are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard is subject to revision at any time by the responsible technical committee and must be reviewed every five years and if not revised, either reapproved or withdrawn. Your comments are invited either for revision of this standard or for additional standards and should be addressed to ASTM International Headquarters. Your comments will receive careful consideration at a meeting of the responsible technical committee, which you may attend. If you feel that your comments have not received a fair hearing you should make your views known to the ASTM Committee on Standards, at the address shown below.