**RELATED TERMS**

- Responder Safety
- Pre-Planning
- Inter-Agency Training

Lessons Learned Information Sharing
www.LLIS.gov

**BEST PRACTICE**

**PRIMARY DISCIPLINES**

- Fire
- Law Enforcement
- Emergency Management

# Incident Site Security: Perimeter Security: Credentialing

## PURPOSE

This Best Practice provides an overview of credentialing procedures for perimeter security at incident sites.

## SUMMARY

This Best Practice discusses the importance of credentialing procedures for incident site security and incident site management. Credentialing procedures help control access to all response areas enclosed by outer perimeters, limiting entry to those tasked by Incident Command (IC). This control prevents complications presented by self-dispatching and volunteerism yet protects responders from secondary attacks. Further, credentialing provides a mechanism to control inner perimeter access.

## DESCRIPTION

Timely access for essential personnel and the prevention of self-dispatch, volunteerism, and unauthorized access are crucial tasks during the initial hours of a response. Credentialing systems help limit access to the incident site(s) to those individuals authorized and dispatched by the IC and/or Unified Command (UC).

Credentialing systems should be pre-designated and universally adopted with a jurisdiction and/or region as standard operating procedures (SOPs) by all responding agencies in order to be effective. Failure to implement credential systems in a prompt manner can lead to site security failures, thus hampering response. Such hindrances put responders, the public, and victims at unnecessary risk.

This Best Practice identifies the core elements of credentialing procedures, including pre-planning, tiers of access, and system flexibility. Emergency planners can use this document when formulating new credentialing procedures or as a reference when evaluating existing systems.

### *Pre-Planning*

Pre-planning of credentialing systems is essential for a number of reasons. Emergency responses to major emergencies usually involve multiple agencies, often spanning several jurisdictions. In the first hours of a response, personnel from numerous agencies will require access to an incident site including fire service personnel, law enforcement, public works or engineering staff, and emergency medical services resources. Similarly, many major all-hazard incidents, and all terrorist incidents, will require a sustained response and comprehensive investigation. This requires a transition from a crude or short-term credentialing system to a more sophisticated one. Interagency pre-planning is required for credentialing systems to ensure access for authorized personnel from disparate agencies, and to facilitate the transition from short-term to long-term credentialing systems. Pre-planning should include protocol development and refinement, interagency training, and periodic exercises to ensure universal familiarity with procedures.

### *Tiers of Access*

Effective incident site security procedures dictate a variety of mechanisms that control outer perimeter access and movement within an incident site across zones of control. Effective credentialing systems must afford outer perimeter access and indicate mission, security clearance, and qualifications to allow movement throughout inner perimeters.

Incident Commanders at the Pentagon used federal identification badges to create a credentialing system within the first few days of the response. While imperfect, this ad hoc system greatly improved access control, and thus, security, safety and accountability concurrently.

Response personnel at the World Trade Center reported confusion and inconsistency at the incident scene as to what constituted credentials for access. Federal Emergency Management Agency health and safety personnel with federal IDs were denied access, while anyone with rescue paraphernalia was admitted immediately.

### Outer Perimeter Access

After an outer perimeter is established, only those personnel tasked by IC and properly credentialed are allowed within the site perimeter. Jurisdictions may employ of variety of identification systems to reflect credentialed status, including cards, armbands, vests, or pre-issued permanent identification cards. In jurisdictions using pre-issued, permanent credentials, law enforcement personnel must be familiar with the system to ensure perimeter security personnel recognize their authority and validity.

The Illinois Statewide Mutual Aid (ISMA) community utilizes reception area procedures to process all personnel and resources during a statewide response. Units authorized by IC are given a verbal security access phrase by a centralized dispatch center. This phrase affords authorized units access to the reception area. Personnel are issued physical credentials in the form of armbands. These armbands are then used to gain access to staging area(s) and incident site(s.)

The National Wildfire Coordination Group (NWCG) maintains standing regional emergency response teams. These teams train and respond as a fully staffed Incident Command System unit, including an Incident Commander, Section Chiefs, and a Safety Officer. Team members are provided with permanent credentials through the National Interagency Fire Center (NIFC) for use during deployment.

The New York City Office of Emergency Management (OEM) stocks pre-made laminate credential cards for use during a major incident requiring access control throughout a sustained response. These cards are issued to authorized personnel at incident staging areas as units arrive. Unique barcodes on each card are scanned upon entry and exit, allowing OEM to account for personnel on site, as well as track hours for reimbursement and insurance purposes.

The US Capitol Police issues prepared ID cards to mutual aid responders as they arrive at the Capitol campus. Perimeter access is authorized on a unit-by-unit basis by the IC via radio communication with access control points. Arriving units proceed to staging areas where personnel are issued temporary ID cards indicating mission and intrasite access. The Capitol Police keep caches of these ID cards to expedite this process.

### Inner Perimeter Authorization, Access to Control Zones

The second essential function of credentialing systems is authorization for movement across the various inner perimeters at the incident site. Effective credentialing systems should clearly indicate levels of access throughout the various control zones. This might be as simple as issuing red ID cards to those personnel authorized to enter the "hot zone," while issuing some other color to all other personnel.

More sophisticated systems will be required for larger and more complex responses. For example, situations with several control zones characterized by different threats (structural, environmental, WMD) and/or security concerns require different indicators of access, including mission qualifications (Urban Search and Rescue, HazMat, disaster medicine, among others.) Many jurisdictions have two, pre-planned credentialing systems: a simple system for use during the short term and a more sophisticated system for use during protracted responses. For example, the Orlando Police Department, in conjunction with the Florida Division of Emergency Management, has contracted the Florida Highway Patrol to provide photo identification cards in the event of a sustained large-scale emergency response.

> The US Capitol Police is responsible for the sensitive information, materials, and historic documents in the Capitol Building and Members' offices. As such, its credentialing system provides access controls for a vast number of inner perimeters required for the protection of these documents and information during a massive emergency response. The US Capitol Police's "Capitol Buildings Emergency Preparedness Program" includes a pre-planned credentialing system that indicates zones of access as well as mission qualifications, credentials, and security clearance.

It is important to note that inner perimeter policing is generally a fire service mission, while credentialing systems will often be a law enforcement task. It is essential that law enforcement planners work with representatives from the fire service and other emergency response organization when developing credentialing systems. All emergency response personnel in a jurisdiction should receive training on the credentialing system. This training can ensure familiarity and foster seamless execution of inner perimeter credential control during a major incident.

### *Flexibility During a Sustained Response*

Credentialing systems should be flexible over the course of a response as operations increase in intensity and complexity. The first hours and days of a major response will be extremely chaotic: credentialing procedures must be dynamic enough to evolve and adapt as the situation develops. Credentialing procedures must account for the constant rotation of personnel, including those subject to credentialing requirements and those enforcing requirements, as well as address the constant flow of new agencies and response organizations integrating into response efforts.

Emergency planners should address the following to ensure the flexibility of credentialing systems:

- **Ongoing Arrival:** Planning for a sustained response must include capabilities to continue to credential personnel as they arrive. If physical credentials (cards, armbands, vests) are stocked for use, planning must include replenishment of the stockpile over the course of a response.
- **Transition from Ad Hoc to Permanent Systems:** Credential-enforcement procedures must allow for a transition from short-term to long-term credentialing.

- **Revocation of Authorization:** Personnel may be dismissed over the course of a response. Credentialing systems must have a mechanism for revocation of site access. In most cases, this can be addressed in a daily briefing system to inform enforcement personnel of any dismissals or revocations of authorization.
- **Limited Public Access:** After the initial response, access to the incident scene by limited personnel may be necessary to maintain continuity of pubic services, critical infrastructure, or businesses. Credentialing systems can include mechanisms that allow limited access to an incident site for personnel deemed critical for continuity of essential operations.
- **Dignitary Access:** Following a major incident, government officials and public figures will often visit the incident site. Emergency planners must expect and plan for these visits. Unique, VIP-specific credentials affording "access-with-escort," which are familiar to all response personnel can be a simple solution to this challenge. Similarly, inner perimeter security personnel must be trained to enforce inner perimeter access requirements for VIPs, including credentials *and* PPE requirements, as they would for any other individual. VIPs at both the Pentagon and the WTC at times did not observe minimum standard PPE requirements, exposing themselves to unnecessary risk.

The Capitol Police "Capitol Building Emergency Response Preparedness Program" includes a program entitled "Fast Facts" (FF). These are updates on procedures and protocol issued each morning and afternoon during a response. FFs include information on dismissals and/or credential revocation. They are issued to every access control point associated with a response and are including in all daily briefings.

Pentagon access was an important issue during the Arlington County response on September 11, 2001. The U.S. Department of Defense had to operate in the midst of a massive emergency response. It took several days to establish an effective system for limited access for essential personnel. Still the *ad hoc* credentialing system changed on a daily basis. The difficulties this variation created emphasized the need for a credentialing system that allowed limited access for essential personnel.

### *The Importance of Training*

Credentialing is a complex and challenging task. Successful implementation of credentialing procedures requires universal familiarity and implementation across all response personnel. Interagency training familiarizes all personnel with credentialing procedures and tests the efficacy of such procedures.

The Illinois State Mutual Aid community put its new credentialing system to the test during the recent Top Officials II Exercise. Its innovative verbal security access-phrase/armband system proved effective in affording access to essential personnel with the appropriate authority while preventing unauthorized access. For more information, please see the *Lessons Learned Information Sharing* Good Story, "Illinois' Statewide Mutual Aid Protocol: Reception Sites."

Business Network of Emergency Resources, Inc. (BNet) is a not-for-profit organization that works with municipalities and private sector businesses to implement emergency credentialing systems. BNet credentials afford critical employees of affected businesses limited access to incident sites to ensure the continuity of business/critical infrastructure.

## RESOURCES

Arlington County, VA. *Arlington County Conference Report: Local Response to Terrorism: Lessons Learned from the 9-11 Attack on the Pentagon*. 01 Nov 2003. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=10355

Department of Homeland Security. *National Incident Management System*. 01 March 2004. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=7975

Federal Emergency Management Agency. *Summary of Post 9/11 Reports "Lessons Learned*." Oct 2002. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=157

International Association of Chiefs of Police*. Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*. Oct 2001. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=6538

International Association of Fire Chiefs. *Performance Capability Recommendations: Second National Conference on Strengthening the Public Safety Response to Terrorism.* 2002. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=8486

Jackson, Brian A., D.J. Peterson, James T. Bartis, et al. *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks.* RAND Science and Technology Policy Institute. 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=7401

McKinsey and Company. *Improving NYPD Emergency Preparedness and Response.* 19 August 2002.
https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=159

McKinsey and Company. *Increasing FDNY's Preparedness.* 01 Aug 2002. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=379

Office for Domestic Preparedness. *Emergency Responder Guidelines.* 01 Aug 2002. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=136

Oklahoma Department of Civil Emergency Management. *After-Action Report: Alfred P. Murrah Federal Building Bombing 19 April 1995 in Oklahoma City, Oklahoma.* Nov 1995. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=6513

Titan Systems Corporation. *Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon.* 30 May 2002. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=483

## DISCLAIMER

This website and its contents are provided for informational purposes only and do not represent the official position of the US Department of Homeland Security or the National Memorial Institute for the Prevention of Terrorism (MIPT) and are provided without warranty or guarantee of any kind. The reader is directed to the following site for a full recitation of this Disclaimer: www.llis.gov.