1   CRISIS EVENT RESPONSE AND RECOVERY ACCESS (CERRA) FRAMEWORK:
2   An Emergency Preparedness Access Implementation and Best Practice Guide
3
4
5   03 August 2017
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

Table of Contents

76

77   Acknowledgements[1]

78   [PLACEHOLDER TO BE COMPLETED FOR FINAL DOCUMENT]

79   This CERRA Framework has been produced in a collaborative effort of the Emergency Services
80   Sector Coordinating Council (ESSCC), in support of the Department of Homeland Security -
81   Office of Infrastructure Protection (DHS/IP), based on identified National Infrastructure
82   Protection Plan (NIPP) priorities.

83

Executive Summary

The capability for local authorities to safely, securely, and effectively control and coordinate the access of key response and recovery resources into an affected area for a crisis event has been identified as a critical success factor in enabling overall community recovery.

The Crisis Event Response and Recovery Access (CERRA) Framework focuses on supporting local, state, and regional efforts to enable the successful transit and access of critical response and recovery resources before, during, and after emergency events. This Framework builds upon prior and existing efforts by the Emergency Services Sector Coordinating Council (ESSCC) and multiple state and local crisis entry access programs to cooperatively define a *common approach* based on best practices to enhance communities' preparation, response, recovery, and resiliency efforts during incident management operations.

This Framework is intended as guidance for government and law enforcement entities. The Framework supports public, private, volunteer and nongovernmental organizations (NGO) in facilitating their response and recovery efforts. It provides mechanisms, tools, and process approaches for coordinating, approving, and enabling access during response and recovery operations. The methods, tools, and templates presented in this Framework are intended to enable governments to define and establish local programs and approaches that can successfully interoperate nationwide.

The CERRA Framework describes a common approach by which communities can:
- Manage and control access for their jurisdiction;
- Develop a consistent, repeatable process to coordinate with organizations that require access to or transit through a restricted area or emergency zone; and
- Coordinate with law enforcement to implement access controls throughout an event.

Introduction

Prior to a natural or manmade disaster, each community should have an emergency preparedness plan to enable response and recovery personnel to conduct incident management and recovery operations. Part of the overall preparedness plan should include a Crisis Event Response and Recovery Access (CERRA) process for managing access into and travel through restricted areas or emergency zones.

The process of managing access into restricted areas or emergency zones during a crisis event is controlled at the state, local, tribal, or territorial level, and can become increasingly difficult when disasters extend across multiple jurisdictions and geographies. In addition, controlling access to affected areas is not only a priority for incident managers and first responders, but also a concern for business owners, critical infrastructure (CI) operators, and community members. The process of granting organizations and individuals access to facilities, businesses, and homes following an incident can substantially add to the level of complexity required to manage the event. These types of operational challenges can directly impact response and recovery timelines and overall operational success. These operational challenges can be overcome by the adoption of a common access and phased entry approach.

Across the nation, those responsible for managing access into emergency zones have experienced delays in response and recovery efforts caused by the lack of common access and phased entry protocols. By adopting the common approach described within the CERRA Framework, jurisdictions will be able to further enhance the access elements of their emergency preparedness plans and accelerate their community's recovery.

This voluntary guidance is not intended as a federal directive to any entity, and nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal, state, or local agencies under statutory authority, nor should this guidance be interpreted as altering or superseding the existing authorities of the laws of any jurisdiction. The CERRA Framework, along with other national preparedness doctrine (e.g., the National Response Framework [NRF] and National Disaster Recovery Framework [NDRF]), provides another tool for common incident management practice.

Purpose

The purpose of this document is to provide state, local, tribal, and territorial (SLTT) governments and their associated entities a framework to guide the implementation of a common approach to manage access requirements when planning for and responding to events and incidents.

Definitions

For the purposes of this document, the following terms and definitions are used.

- **Access**[2,3] refers to the entry to an incident scene, an incident-affected area, or the controlled or restricted roadways supporting the incident.
- **Access Program** refers to the process and technology to enable access.
- **Access Authorization**[4] refers to the procedures and systems defined by state and local authorities to allow access. Access Authorization, when applied in terms of attribute-based access control (ABAC)[5], may be based on required **identification**, **credentials**, **permissions**, or **organizational affiliation**.
- **Access Checkpoint** refers to the point of access, normally managed by law enforcement, into a restricted area or emergency zone.
- **Access Token** refers to the defined visual and electronic standards used for approval of access into a restricted area or emergency zone. Based on jurisdictional access rules visual and/or electronic tokens, to include **access cards**, **letters of access**, and **vehicle placards**, may be used for access control.
- **Crisis or Emergency Event** refers to any incident (manmade or natural), identified by an approved authority (e.g., an Emergency Manager) that requires a coordinated response effort, including the establishment of access control procedures.
- **Emergency Zone** refers to a geographically-defined area that is affected, or is expected to be affected, by an emergency event.
- **Governance Board** refers to the body or group of individuals that have oversight over a local, state, or regional access program.
- **Phased Entry**[6] refers to the process of managing access into a restricted area or emergency zone, before and during response and recovery operations, by categorizing response and recovery assets (e.g. first responders and other incident management personnel, local business owners and utility operators, community members, etc.) into defined functional groups, and coordinating access via defined access levels or tiers.
- **Tiers** refer to jurisdictionally defined access levels. Tier definition may be defined by placement of specified functional groups within each tier based on response and recovery requirements or safety considerations for a given incident. (e.g. A "Tier 1 – HAZMAT" may require personnel to have specific hazardous material [HAZMAT] related skills and defer other Tier 1 resources to another access tier due to their lack of specific training or certification.
- **Restricted Area** refers to a geographical area within a jurisdiction (e.g., an Emergency Zone) in which authorized government officials have restricted access to maintain public safety.

---

[2] FEMA NIMS Guidelines for the Credentialing of Personnel, August 2011.

[3] FEMA Planning Considerations for Access and Re-entry, 2017.

[4] FEMA NIMS Guidelines for the Credentialing of Personnel, August 2011.

[5] NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014.

[6] FEMA Planning Considerations for Access and Re-entry, 2017.

Common Approach

Overview

The CERRA Framework has been developed to enable SLTT jurisdictions to establish their own access programs utilizing a common process approach, recommended best practices, and standard tools and terminology. It is intended that jurisdictions utilize this Framework as a template or operational model to enable coordinated access procedures not only within their jurisdiction for limited size events, but also across multiple jurisdictions during large scale events to effectively support emergency management operations, including protection and restoration of CI, municipal and community lifelines, and public safety.

In addition, this document is meant to complement and expand upon the Federal Emergency Management Agency (FEMA) *Planning Considerations for Access and Re-entry*.

Operational Concept

The challenge facing communities managing access during an event is one of complexity and coordination. Emergency events, by definition, are disruptive. Use of an access program enables a coordinated effort across multiple response and recovery organizations and stakeholders to define:

- Restricted areas – WHERE access restrictions need to be put in place and entry controlled;
- Access Rules – WHO, WHICH and WHEN personnel may enter; and,
- Access Authorization procedures – HOW personnel may gain access.

Representative use-cases are included in Appendix A to illustrate these points. Figure 1 below introduces the different stakeholder communities crucial to access solutions.
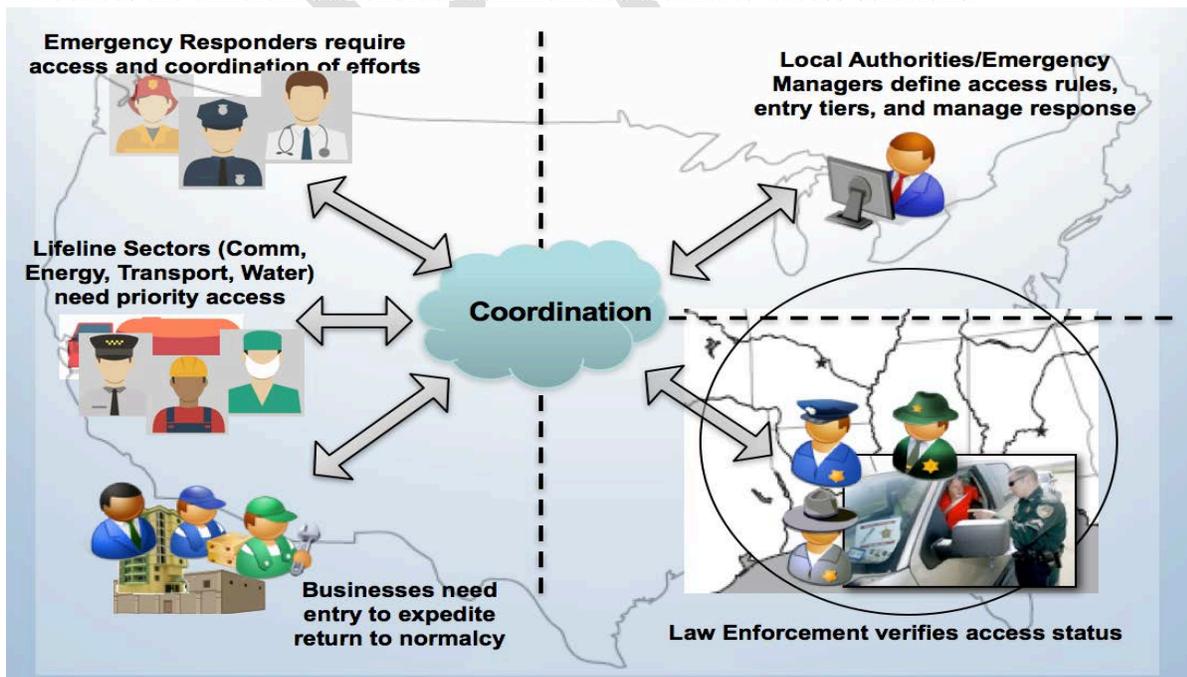

Figure 1: CERRA Stakeholder Coordination Requirements

8

Key Components and Best Practices

The successful implementation of an access program is a combination of (a) prior planning, (b) well defined access protocols and implementation procedures, and (c) tools to facilitate informing and educating incident affected stakeholders and responders. SLTT jurisdictions should detail their access program in an access plan or access program instruction.

The following sections are organized to:

(1) Outline the recommended key components necessary to establish an access program;
(2) Identify recommended best practices to enable program success; and,
(3) Discuss pertinent access planning considerations pertaining to CI response and recovery stakeholders.

Definition of Authority

Jurisdictions interested in establishing an access program should first review their locally defined lines of authority and existing control and management procedures regarding the establishment of access restrictions during emergency events.

> **BEST PRACTICE:** Confirm the state and local authority to establish and operate an access program.

The authority to issue evacuation orders and establish access criteria traditionally exists with a state Governor, but may be the authority of local government leaders. Governors often delegate this authority to local officials, and this delegation may be codified by local statutes or ordinances. During most instances the responsibility and authority for determining the access status, requirements, and permissions necessary to enter a restricted area, rests with the designated local official within the affected jurisdiction.

Depending on the type of event or local statutes, senior officials may elect to delegate the required authorities to the local emergency manager, sheriff, police chief, or fire chief. An access plan or access program instruction should clearly define the process for delegating authority and explain the extent of such authority.

However, in some communities, local officials do not have the legal authority to evacuate a residential area fully, while others may require a disaster declaration before the jurisdictional authority can institute a mandatory evacuation. Understanding the definition of authority to issue evacuation orders and establish access criteria allows communities to better prepare alternatives and plans prior to an incident occurring.

Roles and Responsibilities

Proper implementation of an access program represents the coordinated efforts of many elements of a community. The access plan and planning considerations need to represent state or local operational requirements, constraints, and security considerations, as well as the interests of key

> **BEST PRACTICE:** Establish a clear, advance understanding of dependencies and potential access coordination requirements of local and regional organizations and CI owners and operators.

9

258 elements of the community. Community officials and emergency planners should meet with
259 public, private, NGO, and volunteer organizations, which may be affected by or potentially assist
260 with an incident, during the planning process to define responsibilities and set reasonable
261 expectations. Emergency managers should ensure they are aware of local or regional CI Sector
262 mutual aid plans, and that these plans are coordinated with other jurisdictions and organizations
263 to support potential resource requirements.
264
265 Community officials and emergency planners should
266 define responsibility for managing access and phased
267 entry during the planning processes. Clear lines of
268 authority, responsibility, and coordination
269 requirements between differing organizations and
270 incident stakeholders should be included in the access
271 program instruction. Incorporation of these critical
272 elements into the access program instruction enables
273 both local and state programs to better interoperate,
274 prevent operational issues, and enhance coordination
275 between all incident-related stakeholders.

> BEST PRACTICE: Access programs require clearly defined roles and responsibilities across response and recovery organizational stakeholders.

276 Once a restricted area and access requirements have
277 been defined and activated, it is typically the
278 responsibility of law enforcement,
279 including augmentation personnel from
280 the state National Guard and other
281 jurisdictions, to enforce restrictions and
282 control access. Law enforcement, in
283 coordination with their respective
284 emergency management agency, should
285 exercise the local access program for
286 routine events in order to maintain
287 familiarity with the program's procedures.

Emergency Support Functions
ESF 1 – Transportation
ESF 2 – Communications
ESF 3 – Public Works and Engineering
ESF 4 – Firefighting
ESF 5 – Emergency Management
ESF 6 – Mass Care, Emergency Assistance, Housing, and Human Services
ESF 7 – Logistics Management and Resource Support
ESF 8 – Public Health and Medical Services
ESF 9 – Search and Rescue
ESF 10 – Oil and Hazardous Materials Response
ESF 11 – Agriculture and Natural Resources
ESF 12 – Energy
ESF 13 – Public Safety and Security
ESF 14 – Superseded by the National Disaster Recovery Framework
ESF 15 – External Affairs

CI Lifeline Sectors
Communications Sector
Energy Sector
Transportation Systems Sector
Water and Wastewater Systems Sector

Establishment of a Governance Board

288 Establishment of a Governance
289 Board
290 The role of a Governance Board is to
291 enable an ongoing forum for defining,
292 coordinating, implementing, and
293 providing oversight of an access program.
294 It is recommended that a State or Local
295 Governance Board consist of
296 representatives from their respective
297 jurisdictions and Emergency Support
298 Functions (ESF), or organizations that
299 represent these functions within their
300 community, as identified in their
301 Emergency Operations Plan. Governance
302 Board membership should be driven by
303 state or local definition of authority, roles

304 and responsibilities, and stakeholder
305 interest in the state or local community
306 (e.g. key CI owners/operators and lifeline
307 sector partners).
308
309 A key to the success of a Governance
310 Board is implementation of an inclusive
311 participation process. Through outreach to
312 public sector, private sector, NGOs, and
313 volunteer organizations, the Governance
314 Board may gain insight into the definition

> BEST PRACTICE: Establish a cooperative forum (i.e. Governance Board) to define, coordinate, implement, and oversee the access program.

315 of operational use-cases and event scenarios that may require use of the access program. By
316 'partnering' with these organizations, the community will develop a more robust view of the
317 critical response and recovery requirements and breadth of skills and personnel needed to
318 effectuate recovery. By leveraging the definition of scenarios and use-cases, stakeholders can
319 establish the access program processes, including phased entry, access authorization, access
320 tokens, and access checkpoints most relevant to meeting the needs of their community.

321 ## Phased Entry/Tiered Access
322 Phased entry is a structured process of granting access to an incident site and other restricted
323 areas by aligning response and recovery personnel and other affected stakeholders (e.g. local
324 business owners, utility operators, community members, etc.) into functional groupings, and
325 managing access via defined tiers. A tier may be granted access into the restricted area, or
326 activated by incident management priorities, on a timeline determined by authorities based on
327 situational response or recovery needs, site or area conditions, and safety concerns.

328 Use of phased entry/tiered access provides
329 the capability for communities to define
330 and pre-plan the order of response and
331 recovery resources authorized for access, as
332 well as ensure a safe and orderly return to
333 an affected area by local citizens.

334 The goal of the access tiers is to:
335   (1) Define access levels (tiers) that can
336   align conditions within the affected
337   area to required response and
338   recovery assets needed throughout
339   the timeline of an emergency event;
340
341   (2) Standardize terminology and visual
342   cues (colors/numbers/shapes
343   associated with the access tokens) to
344   support an efficient and effective
345   access control process; and

ER	EMERGENCY RESPONSE: Emergency Zone is unstable – Emergency Services Only
Tier 1	RESPONSE SUPPORT – Zone not stable. Key Resources for relief, assessment, stabilization
Tier 2	RECOVERY SUPPORT: Zone is stable – Support for infrastructure, business recovery & restart
Tier 3	GENERAL RETURN: Zone is stable. Return of Local Community, including use for Curfew Access

Figure 2: Summary Tiered Access Definition

346   (3) Enable specific or additional access requirements as the incident response dictates (e.g.
347   Tier 1[HAZMAT] may delineate that HAZMAT certification is required for access).
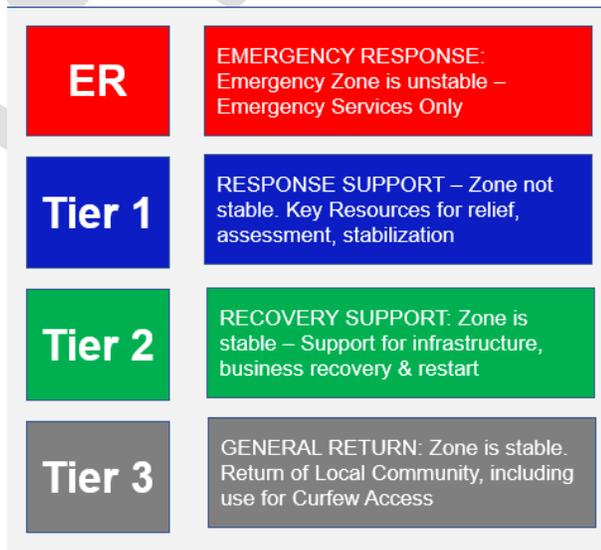
348 During an incident, response and recovery organizations may have personnel who require access
349 across multiple tiers depending on the role(s) and responsibilities required. (E.g. Utilities may
350 require access to facilitate response efforts.
351 Commercial facilities may require access to relieve
352 personnel onsite, provide security, or conduct
353 facility shutdown procedures.) The objective of the
354 tiered access approach is to enable jurisdictions
355 and their response and recovery organizations to
356 map entry of required personnel to access
357 privileges as needed and effect a safe return of
358 community members.
359
360 Although different efforts throughout the United States have implemented similar tiered access
361 methodologies, the ability to align terminology and structure under a common approach will
362 provide substantial benefits to state and local access programs, and can facilitate greater
363 interoperability across jurisdictions nationwide. A proposed tiered access structure is shown in
364 Figure. 2[7] with more detailed information in Appendix B.

Access Authorization

366 A challenge of coordinated access is providing a
367 simple mechanism to approve and permit personnel
368 access to restricted incident areas.

369 An access authorization structure that relies on the
370 definition of validated attributes (e.g.
371 identification, credentials, organizational
372 affiliation, etc.) to enforce the access approval
373 provides local programs with a wide range of
374 control to ensure that only personnel who are
375 approved and meet the established requirements are allowed access. The goal of such an
376 approach focuses on simplifying the capability to coordinate with the organizations requiring
377 access and the law enforcement entities enforcing the defined tiered access levels.

378 An access authorization structure consists of defining standard processes augmented with the
379 definition of jurisdiction, or environment-specific, requirements to provide the level of control
380 for response and recovery as determined by the organization responsible for managing access.
381 Access authorization may leverage existing processes and systems that can provide the level of
382 reliance and capability to the access decision. These may include existing CI sector specific
383 credentials (e.g. Transportation Worker Identification Credential [TWIC] card) or other systems
384 that provide secure identification and credentialing functions. Some jurisdictions may utilize a
385 third party provider to act as a trusted agent or authoritative source to manage and validate
386 predefined access attributes (e.g. verification of identity, employment, certification, etc.) to assist
387 the jurisdiction in making the access decision.
388

BEST PRACTICE: Implement a phased entry access program using a tiered access methodology

BEST PRACTICE: Leverage common access authorization rule sets for standard tier access to facilitate interoperability with other jurisdictions.

---

[7] Copyright protected. See footnote 1.

Access Tokens

Access tokens are paper-based, identification (ID) card based, or electronic-based elements (e.g. vehicle placards and letter of access; recognized credentials and access cards; mobile tokens) used at access checkpoints to enable law enforcement to validate approval for access.

> **BEST PRACTICE:** Utilize a standard set of access tokens to support local jurisdictional access programs.

Use of standard access tokens assists in standardizing operational procedures for validating access permissions across incident-related checkpoints, and provides for a common, secure, and effective mechanism to manage phased entry of resources into an affected area, while enabling flexibility and interoperability with other jurisdictions. Local jurisdictions may tailor access tokens to incorporate additional elements (i.e. local requirements) for specific incidents or to enable interoperability with other jurisdictions. Any such tailored token elements should be coordinated with all relevant jurisdictions, private sector partners, and State entities, as required in order to maintain stakeholder situational awareness. Appendix C provides recommended templates for access tokens formats.

Access Checkpoint Definition

Access Checkpoints are the locations utilized by law enforcement to enable the access or denial of individuals and resources into restricted areas or emergency zones during crisis events. Checkpoint operations, structure, and processes are defined and established by law enforcement. Checkpoints are typically manned by law enforcement personnel, but may be augmented by National Guard, and in some cases private security, personnel. The following provides an outline of potential checkpoint models.

> **BEST PRACTICE:** Define, document, train, and communicate standard processes to establish, manage, and operate checkpoints.

Outer Perimeter Checkpoint

Outer Perimeter Checkpoints are established outside of the emergency zones at a sufficient distance to facilitate restricting access of unapproved personnel and resources. Law enforcement, in conjunction with emergency management personnel, should consider establishing these checkpoints to provide both a buffer around the actual emergency zone and a clear flow of access for response and recovery personnel. Characteristics of an Outer Perimeter Checkpoint may include:

- A location where traffic management is a priority and risk from the incident to response and recovery personnel is relatively low.
- A location suitable to allow for a cursory review of an individual and his or her vehicle by checkpoint personnel (i.e. law enforcement, National Guard, or private security). A visual inspection of a vehicle placard may be sufficient for entry.
- An area or roadway large enough where vehicle placards can be leveraged to form multiple lanes of traffic segmented by access priority (e.g. no placard vs. placard or tier access levels).

431 • An area where individuals can be directed to a secondary area nearby or rerouted to the
432 command post, or staging area, for a further, more detailed review as needed.
433 • Co-located with a designated staging area.
434

435 ## Inner Perimeter Checkpoint
436 Inner Perimeter Checkpoints are recommended to be established at or near the boundary of the
437 emergency zone as a mechanism to control access into and out of the restricted area by approved
438 personnel and resources. Law enforcement, in conjunction with emergency management
439 personnel, should consider establishing these checkpoints to both facilitate efficient access to
440 critical areas and support establishment of secure areas to protect the community and personnel.
441 Characteristics of an Inner Perimeter Checkpoint may include:
442 • A location where risk to response and recovery personnel is higher than at the Outer
443 Perimeter Checkpoint, due to proximity to the incident or ability to move to a safer area
444 quickly.
445 • A location where a more detailed or scrutinized review of a person's identity and
446 verification documents is appropriate.
447 • A visual or electronic inspection of access tokens or verification by checkpoint personnel
448 of an individual's information contained in the access program system.
449
450 Local jurisdictions with limited staffing numbers in the initial wake of an incident may struggle
451 to achieve both an outer and an inner perimeter. These jurisdictions should combine the
452 requirements of both the inner and outer perimeters, (or indeed the most essential requirements
453 of each perimeter), in order to best control access and security with limited available resources.

454 ## Spot Checks
455 Law Enforcement personnel may conduct random spot checks of access tokens throughout an
456 emergency event to maintain security and public safety. Characteristics of a Spot Check may
457 include:
458 • A more detailed or scrutinized review of an individual's access tokens or access program
459 record in the access control system.
460 • May occur in any location throughout the restricted area or emergency zone, to include
461 designated mustering points or staging areas.
462 • May occur at the discretion of law enforcement personnel, prompted by a person's
463 suspicious behavior or geographic location within the emergency zone or restricted area.
464 • An increased risk to law enforcement personnel, when engaging unauthorized or
465 distressed individuals.
466
467 ## Access Program Coordination
468 The implementation of an access program is a complex affair requiring the coordination,
469 cooperation, and integration of multiple government, private sector, and NGOs/Volunteer
470 groups. To facilitate an effective, efficient, and interoperable access program that promotes
471 "whole community" recovery, state and local officials should ensure their access program is
472 capable of:

473 • Providing management, communication, and coordination of locally defined access
474   authorization processes and attribute-based access control criteria to facilitate access before,
475   during, and after an incident;

476 • Registering organizations desiring to pre-enroll in the access program before an incident, as
477   well as a just-in-time enrollment capability for use during incidents;

478 • Providing for multiple delivery
479   methods (e.g. primary – electronic;
480   secondary – paper distribution) of
481   access tokens to enabled efficient
482   access management; and

483 • Conducting widespread outreach and
484   education regarding the access
485   program to all stakeholders including
486   government, law enforcement,
487   businesses, and residents.

488
489

BEST PRACTICE: Establish an ongoing process to manage, update, coordinate, and educate the community and private sector partners on the access program. Consider engaging local, state, or regional business emergency operation centers.

490 # Conclusion
491 [To be completed after WG Review.]

492

Appendix A: Use-Case Examples

Use Case 1: Chemical Facility Response & Recovery

Challenge: Coordination of access management and control for a critical manufacturing facility.

Scenario: A local chemical facility has a robust response and recovery plan in place. During a severe weather emergency, the plant manager ceases operations and evacuates the facility to protect personnel. The only personnel who remain are critical security and operations members (i.e. a ride-out crew.) Extreme damage from the storm requires the local jurisdiction to activate its access control program, defining an emergency zone that includes the chemical plant and establishing Tier ER (Response personnel only) access protocols. Initial assessment by the plant personnel reveals minor damage onsite, but current conditions outside the plant include loss of electrical power, significant flooding, and widespread tree damage impacting local roads. Due to the widespread nature of the damage, surrounding jurisdictions activated similar access programs at the next level of access, Tier 1 (Response Support.)

Operational Challenges:

(1) The Chemical facility needs to send Relief personnel to the facility to maintain security and augment onsite staff until recovery and facility restart operations can commence.

(2) The Chemical company has activated one of its national ER teams to support response and recovery of the facility as the lack of power and flooding have increased the chance for dangerous chemical release. These trained and certified personnel have the experience and resources to react and respond to any potential damage or issue at the facility. They are traveling from outside the state and expect to be onsite within four (4) hours.

(3) Once the emergency zone has been stabilized, the facility staff will activate defined restart teams (including employees and contractors) to assess conditions and begin restart operations. The unexpected shutdown is a costly activity and recovery to full capability is an economic imperative for the organization.

Access Challenges:

(1) The immediate relief crew, although *not* local ER personnel, will need approval to gain access to the restricted zone. These personnel can be pre-enrolled in the local access program, selected by the chemical facility, and approved by the local jurisdiction for access.

(2) Most of the national ER team members selected for this response have been pre-enrolled in the local access program, but two members require just-in-time enrollment, approval, and delivery of Tier ER access tokens.

(3) The programs in the surrounding jurisdictions must accept and recognize the access tokens for the relief and ER response teams to enable access. Since the surrounding jurisdictions have established a 'higher' (less restrictive) condition, if the programs interoperate, the personnel will be approved for access and transit.

(4) The chemical facility team must activate their recovery/restart personnel and ensure the delivery of access tokens. These personnel will be traveling to the facility from multiple locations (home/staging area(s)) and delayed arrival of some members may impact the recovery/restart activities.

537 Based on actual implementation experience and lessons learned, the following is recommended:

538   •   The local (and state) access programs engage and coordinate with the chemical facility
539   (via their governance board) to define and plan for these types of potential response
540   scenarios.
541   •   The chemical facility has enrolled known ride-out, relief, response, and recovery
542   personnel into the access program to facilitate immediate activation and issuance of
543   access tokens.
544   •   The chemical company has enrolled its national response and recovery teams to ensure,
545   upon activation, the personnel could travel from any location and gain access to the
546   jurisdiction.
547   •   The chemical facility worked with the local (and state) access programs to define
548   'special' Tier ER and Tier 1 access levels for chemical and hazardous material spills to
549   support potential spill/release events that impacted the local community.
550   •   The state established a statewide approach and worked with the local jurisdictions
551   (counties) to implement common interoperable access programs. This approach
552   facilitated the ability for response and recovery personnel to move across jurisdictions
553   seamlessly.
554   •   The local program provided mechanisms for just-in-time enrollment and activation by
555   previously registered organizations to enable adding personnel and enabling access.
556
557 Summary: Crisis event response and recovery is dynamic. Pre-planning and preparation provide
558 solid process and coordination capabilities, but the actual execution of response and recovery
559 activities will present unforeseen challenges. The objective of the access program should be to
560 provide mechanisms to react to any scenario through tools and coordination amongst the parties.
561

562 **Use Case 2: Urban Utility Explosion**

563 Challenge: Coordination of access management and control within a dense urban area with
564 substantial high-value economic assets.

565 Scenario: Within a large, highly populated urban area, a utility facility experiences a catastrophic
566 mechanical failure resulting in an explosion, fire, loss of power, as well as significant damage to
567 the surrounding buildings and the underlying utility infrastructure. The impact area is a square
568 area of four (4) by four (4) city blocks surrounding the facility.

569 Emergency response assets react to the event to extinguish the fires, secure and stabilize the
570 facility, begin search and rescue operations, and conduct an assessment of the surrounding area.
571 The surrounding buildings are evacuated leaving only critical security and emergency staff
572 onsite. Injured persons are transported to local hospitals.

573 The level of damage from the event requires the local authorities to establish an emergency zone,
574 activate its access control program, and order an evacuation or nearby residents.

575 Operational Challenges:

576   (1) Establishing control of the incident scene and surrounding area under unified incident
577   command. The complex nature of the incident makes securing the scene and surrounding
578   access points as quickly as possible a priority.

579   (2) Assuming the incident is an accident (i.e. not criminally or terrorism related), the priority
580   for the utility organization and supporting contractors will be to get personnel, most
581   likely from outside the immediate area, to the scene to support securing, stabilizing, and
582   assessing damage. These utility crews have specialized training and skills to deal with the
583   incident, but may not be easily distinguishable to law enforcement enforcing the access
584   points. Speedy access to the damaged facility will be critical to minimizing further impact
585   and effecting restoration. The utility crews can be expected on site within hours of the
586   event.
587   (3) Once the event has been stabilized, the surrounding facilities will require their own
588   response, assessment, and other specialized personnel to enter the area. These businesses
589   may have critical operations or materials that require monitoring and onsite personnel
590   who may need relief. Controlling access to these facilities through one or two access
591   perimeters will be challenging given the personnel are not traditional emergency
592   responders, but fulfilling a role critical to the overall economic health of the community.
593
594 Access Challenges:

595   (1) The utility crews and subcontractors, although *not* local ER personnel, will need approval
596   to gain access to the restricted area. These personnel can be pre-enrolled in the local
597   access program, selected by the utility, and approved for access. Some individuals may
598   require just-in-time enrollment, approval, and delivery of the tier access tokens.
599   (2) The density of the urban environment will compress the distances and transit times
600   between zones, creating both potential for gridlock and congestion. The ability for the
601   access control areas to be quickly established and communicated will facilitate smoother
602   transit to and from the zones.
603   (3) The challenge of managing and tracking response and recovery personnel is increased by
604   the complex nature of the overall event. Personnel needed to conduct initial damage
605   assessments will require access (e.g. structural engineers to inspect buildings;
606   communication/IT engineers to restore/repair communications). The personnel,
607   organizations, and potential suppliers who support these functions may not be 'known' to
608   the local access program ahead of time and may require just-in-time access.
609   (4) In all response and recovery activities, the logistical movement of equipment and
610   supplies is a critical success factor. Transportation personnel (i.e. trucking) may well not
611   be known ahead of time to the local authorities. Providing reliable access mechanisms for
612   these personnel (and their resources) is crucial.
613
614 Based on actual implementation experience and lessons learned, the following is recommended:

615   • The local access program manager should engage local CI stakeholders to discuss
616   potential response scenarios and access requirements. This preparation enables the
617   jurisdiction to 'activate' its access program and establish geographic boundaries quickly.
618   • The local access program manager should engage local business, CI facilities, and other
619   organizations throughout the jurisdiction to encourage pre-registration and enrollment of
620   personnel who may require access during an event.
621   • The local access program establishes a mass communication approach for response and
622   recovery personnel, as well as local residents and non-essential workers. Keeping non-

623 approved personnel away from the event scene is as critical as facilitating access of
624 approved personnel.
625 • Establish an interoperable access program framework to enable response and recovery
626 personnel from outside the jurisdiction to quickly gain approval to enter.
627 • Provide mechanisms for just-in-time enrollment and additional access enrollment by
628 previously registered organizations.
629
630 Summary: Urban events amplify many of the issues surrounding crisis event response. The shear
631 density of the environment and need to facilitate evacuation, securing the scene, and setting
632 restricted areas will stress the local program and personnel. Crisis event response and recovery is
633 dynamic. Pre-planning and preparation provide solid processes and coordination capabilities, but
634 the actual execution of response and recovery activities will present unforeseen challenges. The
635 objective of the access program should be to provide mechanisms to react to any scenario
636 through tools and coordination amongst the parties.
637

638 **Use Case 3: Impact to Community Healthcare Resources**

639 Challenge: Coordination of access management and control during crisis events to secure and
640 support critical community healthcare resources.

641 Scenario: A significant or geographically wide spread crisis event has occurred. Local authorities
642 have established checkpoints to restrict access to the emergency zone. Due to the influx of
643 patients to local hospitals, pre-existing community healthcare needs (e.g. requirements for in-
644 home and long-term care services), and the enforcement of access control measures, regional and
645 local healthcare facilities' operating capacities are stressed or severely strained.

646 Critical to the ability for a community, region, or state to successfully react and respond to a
647 crisis event, is the capability to maintain operations and community support activities by local
648 hospitals. During crisis events, especially when an evacuation or restricted access is in effect,
649 hospital environments may become over stressed, as other components of the community's
650 healthcare system and support structure (e.g. outpatient facilities, patient transportation
651 companies, medical equipment and pharmaceutical suppliers, utility providers, etc.) are
652 interrupted or unable to provide services.

653 In these environments, it is crucial for communities to maintain the operations of local hospitals
654 or restore these facilities and supporting infrastructure as quickly as possible. Unfortunately,
655 unlike many other facilities, hospitals cannot operate with limited staff and often require normal
656 staffing plus augmentation personnel to achieve the level of operations necessary to support a
657 crisis event. In addition, hospitals require a near-continuous flow of logistical support to meet
658 their operational requirements.

659 Operational Challenges:

660 (1) Maintaining operations before, during, and after crisis events may require additional
661 personnel from existing hospital staff or augmentation from other medical facilities.
662 These individuals will be going *towards* or into a restricted area to perform critical
663 activities, but may not meet the expected definition of an emergency response individual.

664   (2) Hospitals operate with full or nearly full staffs, which provide many support and
665   administrative roles outside of traditional emergency responder definitions. Ensuring the
666   availability of these staff members is critical to maintaining operations.
667   (3) Hospital and State ESF-8 plans often include the steps to identify qualified and licensed
668   augmentation staff (e.g. doctors, nurses, specialized healthcare providers, ambulatory
669   care, etc.) to provide support to medical facilities during events. These personnel may be
670   identified *after* the event and travel to the facility via their personal vehicle (POV).
671   Ensuring these 'authorized' personnel have access is critical to maintaining operations.
672   (4) Hospitals require near continuous receipt of supplies during events to support the increase
673   operating tempos and workloads. This requires the expedited entry of logistical resources
674   and healthcare related service providers.
675
676 Access Challenges:

677   (1) Ensuring access coordination across all elements of the community's healthcare system
678   and support structure is key to maintaining hospital operations and providing for other
679   community healthcare needs.
680   (2) Ensuring the access of key personnel to maintain required staffing levels for hospitals and
681   other essential healthcare facilities (e.g. dialysis centers) requires close integration with
682   the local access program.
683   (3) Providing access tokens to approved augmentation personnel, who may not be pre-
684   registered or known to the access program.
685   (4) Ensuring the ability to identify and support access of critical healthcare suppliers.
686
687 Based on actual implementation experience and lessons learned, the following is recommended:

688   • Hospitals, along with all the other elements of a community's healthcare support
689   structure, form a key lynchpin in the overall healthcare resilience posture for a
690   community or state. Engaging at both the local and state level to incorporate a consistent
691   and interoperable approach to support access requirements for hospitals is a
692   recommended best practice.
693   • Access program managers, should work jointly with their local hospitals, state health and
694   public healthcare, and ESF-8 organizations, and appropriate licensing boards to establish
695   a coordinated response process to ensure that augmentation personnel can be quickly
696   identified, authorized, and delivered access tokens to expedited their transit and arrival to
697   designated facilities.
698   • Hospital suppliers serve multiple communities across the country and may often re-route
699   deliveries to impacted areas to shorten the response time. The capability of local
700   communities to react and approve access with a consistent and interoperable approach
701   facilitates their support.
702

703 Summary: The healthcare pyramid within the United States is 'anchored' by the hospital unit
704 within a community. The ability to maintain hospital operations during and after a crisis event is
705 critical for a community to successfully react and recover. Tight integration with the access
706 program is a key requirement.

707

708

709 **Appendix B: Tier Access Definition (Draft)[8]**

Tier	Situation	Access Considerations
Tier ER **Emergency Response** 🟥 RED	**TIMEFRAME:** During and immediately after emergency event **EMERGENCY ZONE:** Area considered potentially hazardous or unstable **AUTHORIZED ACCESS:** Local first responders and other approved emergency response personnel after visual inspection of approved forms of ID or Tier ER access tokens	• Specific or additional access restrictions required (e.g. Tier 1[HAZMAT]) • Critical Infrastructure related personnel may require access (e.g. utility crews, hospital staff, supporting transportation assets, etc.) • Status of Evacuation (pending, ordered or underway) • Establishment of Inner and Outer Perimeter Checkpoints
Tier One (1) **Response Support** 🟦 BLUE	**TIMEFRAME:** Before and After Emergency Event **EMERGENCY ZONE:** Area not stabilized for general entry; Potential hazardous conditions may still exist **AUTHORIZED ACCESS:** Tier ER support and relief assets, utility crews, hospital staff, transportation assets, CI relief personnel and inspection teams, and other approved response resources after visual inspection of approved forms of ID and access tokens	• Priority to response resources needed • Safety of response personnel • Hazards within designated restricted areas • Status of Evacuation (pending, ordered, or underway) • Access token required for non-marked or personal vehicles • Location of staging areas • Coordination with checkpoint personnel
Tier Two (2) **Recovery Support** 🟩 GREEN	**TIMEFRAME:** After Emergency Event **EMERGENCY ZONE:** Area stabilized for entry of repair/recovery personnel; Potential hazardous areas may still exist **AUTHORIZED ACCESS:** Response and recovery support personnel – not general population (e.g. business owners, private sector inspection and repair crews, NGO and volunteer organizations, etc.) after visual inspection of approved forms of ID and access tokens.	• Priority to resources required for reestablishing essential services • Safety of response and recovery personnel • Spot Checks within restricted areas • Access tokens required for non-marked or personal vehicles • Location of staging areas • Coordination with checkpoint personnel
Tier Three (3) **General Return** ⬛ GREY	**TIMEFRAME:** After Emergency Event **EMERGENCY ZONE:** Area stabilized for general entry (Safe travel for civilians); Basic lifeline services restoration in process. **AUTHORIZED ACCESS:** Local residents, community members, and non-essential personnel after visual inspection of approved forms of ID and access tokens.	• Any jurisdictional curfew restrictions • Any Checkpoints being maintained • Any remaining hazards or designated restricted areas • Access tokens required for non-marked or personal vehicles •

710

---

[8] Used with permission. See Note 1.

Appendix C: Access Token Definition Sample (Vehicle Placard/Letter of Access)[9]

Tier 2 All Hazards Depicted. Adjust accordingly, including corresponding color banners and Tier designation, for other tiers. Font sizes must be as large as possible while still fitting in text.

- Placard shall have a ½" margin. All fonts shall be "Arial Black" and Bolded, all capitalized and shall be a minimum of 24pt font size, except for the Tier and ESF Indicator Zones.
- Event Name and Purpose / Destination Zone shall be white colored text on the corresponding tier color background (bounding box 8" (w) by 1.5" (h))
- The Tier Designator zone shall be 2" (w) x 1.5" (h) in size and have the corresponding tier color background. The font for the letters "ER" or the numerical digit ("1", "2", or "3") shall be 80pt font size, white in color and do not have to be bolded. The color will be spelled out directly underneath and shall be 20pt font size.
- ESF Indicator Zone / icon shall be 2" (w) by 1.5" (h) in size and include the letters "ESF" and the ESF numerical digit (26pt font size.)
- The unique number shall appear in between the two logos, rotated 90° counter-clockwise.
- A two (2) digit YEAR will be displayed above the Tier banner in white on a white field (e.g. "12")
- A QR Code will be included between the logos. The QR code will include the Placard data in full.
- OPTIONAL: A State-specific defined barcode (PDF-417 is displayed below) may be added at the direction of the State Governance Board
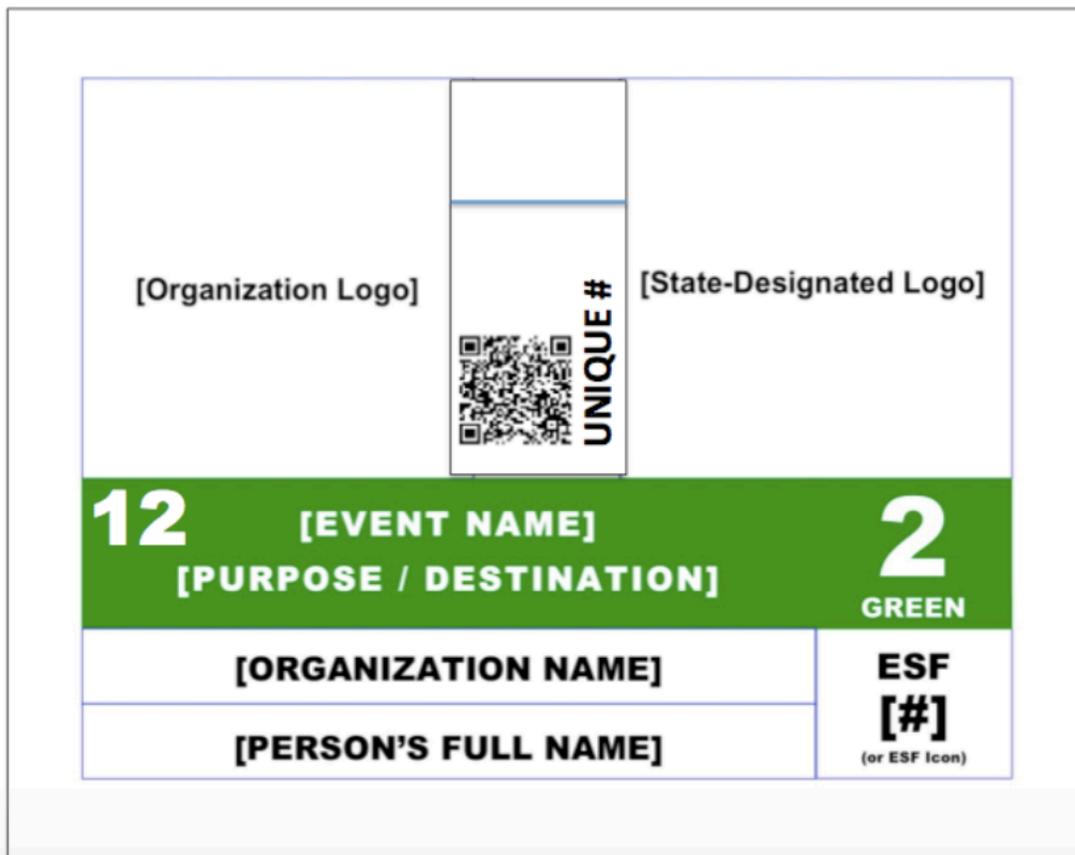

713

---

[9] Used with permission. See Note 1.

714

Tier 2 All Hazards Depicted. Adjust accordingly, including corresponding color banners and Tier designation, for other tiers. Font sizes must be as large as possible while still fitting in text.

- All fonts shall be "Arial Black" and Bolded
- Event Name, Purpose/Destination, Organization Name and Person's Full Name shall be Bold, Arial Black font and 14pt in size, white in color with the corresponding tier color background.
- Letter Body, Manager's Contact Info and Person-Specific Zone must be Arial 11pt font (bolded font not necessary)
- Tier Designator text shall be a minimum of 48pt in size, white in color with the corresponding tier color background. The color name will appear underneath in 12pt Arial Black font, white in color.

715
716
717
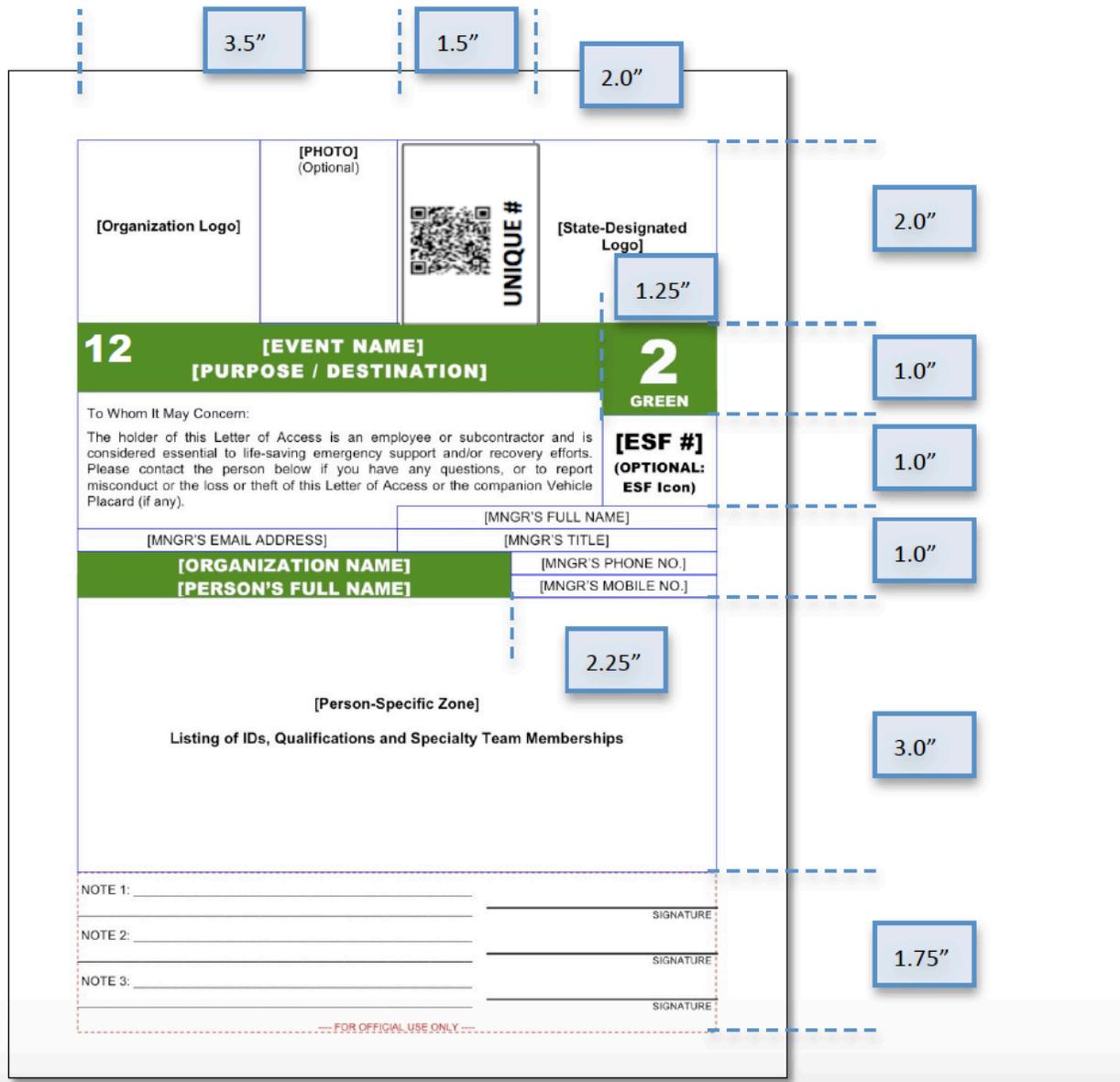
Appendix D: Sector Specific Access Planning Considerations

The following are CI Sector stakeholder recommended access planning considerations that community officials and emergency planners should be aware of when developing and executing an access program.

Emergency Services Sector

- During an incident, local, regional, or state officials may have to deal with a number of business owners and citizens who refused to comply with issued evacuation orders. This type of situation may create a perception that some persons were allowed to re-enter the restricted area or emergency zone, while others were not. In addition, this situation poses an uncontrolled security and safety risk to both first responders and recovery personnel. Community officials and emergency planners should consider this operational challenge when developing incident management plans.

Water and Wastewater Sector

- During incidents, some sector mutual aid agreements, such as the Water/Wastewater Agency Response Networks (WARNs), may involve movement of resources among several jurisdictions and access issues should be coordinated ahead of time.
- During emergencies, water utility personnel need the same degree of access as other first responders to maintain a community's protective and lifeline facilities (e.g. water utility personnel often need access to pump stations even though they may not be directly involved in the emergency response portion of an event).

Transportation Sector

- Within the trucking industry, the two primary credentials truck drivers may possess are the RealID compliant Commercial Drivers' License (CDL) and the Transportation Worker Identification Credential (TWIC). Individuals issued one of these credentials have undergone a rigorous security vetting process to verify identity, criminal history, and professional qualifications. Possession of one of these forms of identification, along with an appropriate bill of lading (BoL), may be sufficient to determine that the driver has legitimate business in the incident area and should be considered for inclusion in the overall access program instruction.
- In some instances, a truck driver may be contracted to provide a service without a BoL (e.g. relocate trailers inside the restricted area) because the items being transported did not originate from a shipper's facility and standard access procedures may apply.

Communications Sector

- During an incident, communications personnel and their contractors require access similar to first responders in order to sustain and recover lifesaving and life sustaining communications services (e.g. 911 emergency calls, first responder communications, and dispatch).
- Communications is an interdependent network of networks. Many companies are involved in handing off traffic between originating and destination parties (e.g. many cellular companies depend upon cable operators to provide backhaul connectivity between cell sites and switching offices); necessitating the need to grant access to multiple entities.

763　　• In some cases, communications infrastructure owner/operators subcontractors require
764　　　access to provide vital services such as generator management, refueling, and roof repair.
765　　　These subcontractors should be afforded the same access courtesies as the
766　　　communications entity they are supporting.
767

Appendix E: Resources

The following resources may assist in access program planning and implementation efforts.

Federal Access-related Resources

- FEMA *Planning Considerations for Access and Re-entry*; dated TBD – provides a series of planning considerations to enable local officials and emergency planners to develop or enhance the access and re-entry elements of their jurisdictions' emergency preparedness plans. (link to be added)
- FEMA *National Incident Management System Guidelines for the Credentialing of Personnel*; dated August 2011 – provides guidance regarding national credentialing standards to Federal agencies with responsibilities under the National Response Framework and provides guidance to all other public and private organizations. (link to be added)

State Credentialing and Access Programs

- Connecticut Statewide Credentialing document – http://www.ct.gov/demhs/cwp/view.asp?a=1928&q=553608&demhsNav=|51600|
- Florida Statewide Private Sector Re-Entry Program – http://www.floridadisaster.org/PublicPrivateSector/reentry_information.html
- Georgia Critical Workforce Disaster Re-entry Permits SOP - http://www.gema.ga.gov/PlanPrepare/Pages/PlansMaps.aspx
- Louisiana Statewide Credentialing and Access Program – http://lwin.la.gov/plans.aspx
- Massachusetts Corporate Emergency Access System Program – http://www.ceas.com/our_programs/ma/
- Mississippi Statewide Emergency Access Program (MEAP) – http://www.dps.state.ms.us/divisions/office-of-emergency-operations/mississippi-statewide-credentialing-access-program/
- New Jersey Private Sector Essential Employee Registration Program – http://www.ready.nj.gov/pdf/101510_essesntialempreg.pdf
- North Carolina Disaster Re-entry Certification Program –
- Ohio Emergency Partner Credentialing System – http://homelandsecurity.ohio.gov/op3.stm
- Rhode Island Corporate Emergency Access System Program – https://www.providenceri.com/PEMA/pema-for-businesses-corporate-emergency-access
- South Carolina Business Reentry Certification Program – http://www.scemd.org/business
- Texas Responder Reentry: State of Texas Emergency Management Plan
- Washington Business Re-Entry Pass system – http://mil.wa.gov/form/business-re-entry-pass
- Wisconsin Credentialing & Asset Management System (WI-CAMS) – http://wicams.wi.gov

Sector Partnership developed resources

- CERRA Baseline Use Cases (To be developed by CERRA WG; link to be added)
- Governance Model reference (To be developed by CERRA WG; link to be added)

Non-profit Access-related Programs

The following are non-profit public-private partnership programs providing no-cost support to jurisdictions operating state, local, or regional access programs.

- Emergency Responder Identity Trust Network (ER-ITN) – https://eritn.com
- Corporate Emergency Access System (CEAS) – http://www.ceas.com

Appendix F: Glossary

For the purpose of the CERRA Framework, the following terms and definitions apply:

Access:[10,11] Refers to the entry to an incident scene, an incident-affected area, or the controlled or restricted roadways (transit) supporting the incident.

Access Control:[12] Refers to the process of granting or denying requests for access.

Access Program refers to the process and technology to enable access.

Access Authorization:[13] Refers to the procedures and systems defined by state and/or local authorities to allow access. Access Authorization, when applied in terms of attribute-based access control (ABAC)[14], may be based upon required attributes, to include:

- **Identification**[15] – The ability to prove identity of an individual via Government-issued and/or Organization-issued identification or credentials (i.e. State Driver's License, Federal ID Card, TSA Transportation Worker Identification Credential [TWIC] card).
- **Credentialing**[16]**,** or **Capability** – Refers to the administrative process for validating or providing, respectively, documentation that identifies personnel and authenticates and verifies the qualifications of such personnel by ensuring that such personnel possess a minimum common level of training, experience, physical and medical fitness, and capability appropriate for a specific position.
  - o **Credential** refers to the artifact (e.g. physical card/document) that represents the credentialing referenced above. A Credential may be used as a valid Access Token, depending on the access rules established by the Jurisdiction.
- **Affiliation or Membership** – Verifiable membership to an organization or group (i.e. an employee of Company ABC).
- **Permission** – The temporal-based approval by the responsible organization to access a restricted area or emergency zone in support of response or recovery operations.

Access Checkpoint: Refers to the point of access, normally managed by law enforcement, into a restricted area or emergency zone.

Access Token: Refers to the defined visual and electronic standards used for approval of access into a restricted area or emergency zone. These may include:

- **Access Card** – Refers to a secure physical card that is used to identify an individual's specific qualification and organizational affiliation.

---

[10] NIMS Guideline for the Credentialing of Personnel, August 2011.

[11] FEMA Planning Considerations for Access and Re-entry, 2017.

[12] NIMS Guideline for the Credentialing of Personnel, August 2011.

[13] NIMS Guideline for the Credentialing of Personnel, August 2011.

[14] NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014.

[15] NIST IR 7298 Revision 2, Glossary of Key Information Security Terms, May 2013.

[16] NIMS Guideline for the Credentialing of Personnel, August 2011, DHS, Page 3.

- **Letter of Access** – Refers to a paper or electronic access token that is used to identify an individual's specific qualification(s) and grant him or her access to a restricted area or emergency zone.
- **Vehicle Placard** – Refers to a paper access token that can be used to identify that an individual(s) traveling by vehicle has been granted access to or permission to transit through a restricted area or emergency zone.

Crisis or Emergency Event: Refers to any incident (manmade or natural), identified by an approved authority (e.g., an Emergency Manager) that requires a coordinated response effort, including the establishment of access control procedures.

Emergency Manager: Refers to a designated individual, or role, authorized to act with jurisdictional authority, which during a crisis, or emergency event, is responsible for incident management at the local and/or state level. (Note: This 'role' may be assigned to law enforcement or fire department depending on the structure and organization of the jurisdiction. The title Emergency Manager may not indicate this delegated authority.)

Emergency Zone: Refers to a geographically-defined area that is affected, or is expected to be affected, by an emergency event.

Enrollment Process: Refers to the establishment of individuals within the CERRA environment. Individual records include 'claims' for Identifications, Affiliations (Memberships), and Credentials/Capabilities for each individual used to satisfy established access rules for entry.

Governance Board: Refers to the body or group of individuals that have oversight over a local, state, or regional access program.

Phased Entry:[17] Refers to the process of managing access into a restricted area or emergency zone, before and during response and recovery operations, by categorizing response and recovery assets (e.g. first responders and other incident management personnel, local business owners and utility operators, community members, etc.) into defined functional groups, and coordinating access via defined access levels or tiers.
- **Tiers** – Refer to jurisdictionally defined access levels. Tier definition may be changeable (i.e. placement of different functional groups within each tier) based on response and recovery requirements or safety considerations for a given incident.

Registration Process: Refers to the process of establishing a trusted organizational entity within the CERRA environment to form 'membership' classes. Organizations may include public, private, NGO, and/or volunteer-based entities and form the Affiliation or Membership link that may be required for access.

Resource: Refers to an individual, vehicle, or other asset that requires access to support response or recovery activities. Resources are often commonly defined in terms of individual personnel, but can also be used to identify specific equipment or supplies involved in response or recovery efforts. (e.g., specialized equipment, logistics trailer)

---

[17] FEMA Planning Considerations for Access and Re-entry, 2017.

883 **Restricted Area:** Refers to a geographical area within a jurisdiction (e.g., an Emergency Zone)
884 in which authorized government officials have restricted access to maintain public safety.

885