CRISIS EVENT RESPONSE AND RECOVERY ACCESS (CERRA) FRAMEWORK:
An Emergency Preparedness Access Implementation and Best Practice Guide

03 August 2017
# Table of Contents

41 Executive Summary................................................................. 5
43 Introduction ............................................................................ 6
44 Purpose .................................................................................... 6
45 Definitions ............................................................................... 7
46 Common Approach ................................................................. 8
47 Overview ................................................................................ 8
48 Operational Concept ............................................................. 8
49 Key Components and Best Practices ................................... 9
50 Definition of Authority ......................................................... 9
51 Roles and Responsibilities .................................................... 9
52 Establishment of a Governance Board ............................... 10
53 Phased Entry/Tiered Access ................................................ 11
54 Access Authorization .............................................................. 12
55 Access Tokens ....................................................................... 13
56 Access Checkpoint Definition ............................................ 13
57 Outer Perimeter Checkpoint ................................................ 13
58 Inner Perimeter Checkpoint ................................................ 14
59 Spot Checks ........................................................................ 14
60 Access Program Coordination ............................................. 14
61 Conclusion ............................................................................. 15
62 Appendix A: Use-Case Examples ........................................ 16
63 Appendix B: Tier Access Definition (Draft) ......................... 21
64 Appendix C: Access Token Definition Sample ................... 22
65 Appendix D: Sector Specific Access Planning Considerations 24
66 Emergency Services Sector .................................................... 24
67 Water and Wastewater Sector .............................................. 24
68 Transportation Sector ............................................................ 24
69 Communications Sector ....................................................... 24
70 Appendix E: Resources ......................................................... 26
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>Federal Access-related Resources</td>
<td>26</td>
</tr>
<tr>
<td>72</td>
<td>State Credentialing and Access Programs</td>
<td>26</td>
</tr>
<tr>
<td>73</td>
<td>Sector Partnership developed resources</td>
<td>26</td>
</tr>
<tr>
<td>74</td>
<td>Non-profit Access-related Programs</td>
<td>26</td>
</tr>
<tr>
<td>75</td>
<td>Appendix F: Glossary</td>
<td>27</td>
</tr>
<tr>
<td>76</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Acknowledgements

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

1 Copyrighted material is included in this document with permission of Pegasus Research Foundation, including “Figure 2: Summary Tiered Access Definition”, “Appendix B: Tier Access Definition”, and “Appendix C: Access Token Definition Sample (Vehicle Placard/Letter of Access)”. All rights reserved.
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.
\(^6\) 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](image)
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.

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 stakeholders.
elements of the community. Community officials and emergency planners should meet with public, private, NGO, and volunteer organizations, which may be affected by or potentially assist with an incident, during the planning process to define responsibilities and set reasonable expectations. Emergency managers should ensure they are aware of local or regional CI Sector mutual aid plans, and that these plans are coordinated with other jurisdictions and organizations to support potential resource requirements.

Community officials and emergency planners should define responsibility for managing access and phased entry during the planning processes. Clear lines of authority, responsibility, and coordination requirements between differing organizations and incident stakeholders should be included in the access program instruction. Incorporation of these critical elements into the access program instruction enables both local and state programs to better interoperate, prevent operational issues, and enhance coordination between all incident-related stakeholders.

Once a restricted area and access requirements have been defined and activated, it is typically the responsibility of law enforcement, including augmentation personnel from the state National Guard and other jurisdictions, to enforce restrictions and control access. Law enforcement, in coordination with their respective emergency management agency, should exercise the local access program for routine events in order to maintain familiarity with the program’s procedures.

Establishment of a Governance Board
The role of a Governance Board is to enable an ongoing forum for defining, coordinating, implementing, and providing oversight of an access program. It is recommended that a State or Local Governance Board consist of representatives from their respective jurisdictions and Emergency Support Functions (ESF), or organizations that represent these functions within their community, as identified in their Emergency Operations Plan. Governance Board membership should be driven by state or local definition of authority, roles

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

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

CI Lifeline Sectors
- Communications Sector
- Energy Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector
and responsibilities, and stakeholder interest in the state or local community (e.g. key CI owners/operators and lifeline sector partners).

A key to the success of a Governance Board is implementation of an inclusive participation process. Through outreach to public sector, private sector, NGOs, and volunteer organizations, the Governance Board may gain insight into the definition of operational use-cases and event scenarios that may require use of the access program. By ‘partnering’ with these organizations, the community will develop a more robust view of the critical response and recovery requirements and breadth of skills and personnel needed to effectuate recovery. By leveraging the definition of scenarios and use-cases, stakeholders can establish the access program processes, including phased entry, access authorization, access tokens, and access checkpoints most relevant to meeting the needs of their community.

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

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

The goal of the access tiers is to:
1. Define access levels (tiers) that can align conditions within the affected area to required response and recovery assets needed throughout the timeline of an emergency event;
2. Standardize terminology and visual cues (colors/numbers/shapes associated with the access tokens) to support an efficient and effective access control process; and
3. Enable specific or additional access requirements as the incident response dictates (e.g. Tier 1[HAZMAT] may delineate that HAZMAT certification is required for access).

Figure 2: Summary Tiered Access Definition
During an incident, response and recovery organizations may have personnel who require access across multiple tiers depending on the role(s) and responsibilities required. (E.g. Utilities may require access to facilitate response efforts. Commercial facilities may require access to relieve personnel onsite, provide security, or conduct facility shutdown procedures.) The objective of the tiered access approach is to enable jurisdictions and their response and recovery organizations to map entry of required personnel to access privileges as needed and effect a safe return of community members.

Although different efforts throughout the United States have implemented similar tiered access methodologies, the ability to align terminology and structure under a common approach will provide substantial benefits to state and local access programs, and can facilitate greater interoperability across jurisdictions nationwide. A proposed tiered access structure is shown in Figure. 27 with more detailed information in Appendix B.

Access Authorization

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

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

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

---

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. 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.

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).
An area where individuals can be directed to a secondary area nearby or rerouted to the command post, or staging area, for a further, more detailed review as needed.

Co-located with a designated staging area.

**Inner Perimeter Checkpoint**

Inner Perimeter Checkpoints are recommended to be established at or near the boundary of the emergency zone as a mechanism to control access into and out of the restricted area by approved personnel and resources. Law enforcement, in conjunction with emergency management personnel, should consider establishing these checkpoints to both facilitate efficient access to critical areas and support establishment of secure areas to protect the community and personnel.

Characteristics of an Inner Perimeter Checkpoint may include:

- A location where risk to response and recovery personnel is higher than at the Outer Perimeter Checkpoint, due to proximity to the incident or ability to move to a safer area quickly.
- A location where a more detailed or scrutinized review of a person’s identity and verification documents is appropriate.
- A visual or electronic inspection of access tokens or verification by checkpoint personnel of an individual’s information contained in the access program system.

Local jurisdictions with limited staffing numbers in the initial wake of an incident may struggle to achieve both an outer and an inner perimeter. These jurisdictions should combine the requirements of both the inner and outer perimeters, (or indeed the most essential requirements of each perimeter), in order to best control access and security with limited available resources.

**Spot Checks**

Law Enforcement personnel may conduct random spot checks of access tokens throughout an emergency event to maintain security and public safety. Characteristics of a Spot Check may include:

- A more detailed or scrutinized review of an individual’s access tokens or access program record in the access control system.
- May occur in any location throughout the restricted area or emergency zone, to include designated mustering points or staging areas.
- May occur at the discretion of law enforcement personnel, prompted by a person’s suspicious behavior or geographic location within the emergency zone or restricted area.
- An increased risk to law enforcement personnel, when engaging unauthorized or distressed individuals.

**Access Program Coordination**

The implementation of an access program is a complex affair requiring the coordination, cooperation, and integration of multiple government, private sector, and NGOs/Volunteer groups. To facilitate an effective, efficient, and interoperable access program that promotes “whole community” recovery, state and local officials should ensure their access program is capable of:
• Providing management, communication, and coordination of locally defined access authorization processes and attribute-based access control criteria to facilitate access before, during, and after an incident;

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

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

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

**Conclusion**

[To be completed after WG Review.]
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.
Based on actual implementation experience and lessons learned, the following is recommended:

- The local (and state) access programs engage and coordinate with the chemical facility (via their governance board) to define and plan for these types of potential response scenarios.
- The chemical facility has enrolled known ride-out, relief, response, and recovery personnel into the access program to facilitate immediate activation and issuance of access tokens.
- The chemical company has enrolled its national response and recovery teams to ensure, upon activation, the personnel could travel from any location and gain access to the jurisdiction.
- The chemical facility worked with the local (and state) access programs to define ‘special’ Tier ER and Tier 1 access levels for chemical and hazardous material spills to support potential spill/release events that impacted the local community.
- The state established a statewide approach and worked with the local jurisdictions (counties) to implement common interoperable access programs. This approach facilitated the ability for response and recovery personnel to move across jurisdictions seamlessly.
- The local program provided mechanisms for just-in-time enrollment and activation by previously registered organizations to enable adding personnel and enabling access.

Summary: Crisis event response and recovery is dynamic. Pre-planning and preparation provide solid process and coordination capabilities, but the actual execution of response and recovery activities will present unforeseen challenges. The objective of the access program should be to provide mechanisms to react to any scenario through tools and coordination amongst the parties.

Use Case 2: Urban Utility Explosion

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

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

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

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

Operational Challenges:

(1) Establishing control of the incident scene and surrounding area under unified incident command. The complex nature of the incident makes securing the scene and surrounding access points as quickly as possible a priority.
Assuming the incident is an accident (i.e. not criminally or terrorism related), the priority for the utility organization and supporting contractors will be to get personnel, most likely from outside the immediate area, to the scene to support securing, stabilizing, and assessing damage. These utility crews have specialized training and skills to deal with the incident, but may not be easily distinguishable to law enforcement enforcing the access points. Speedy access to the damaged facility will be critical to minimizing further impact and effecting restoration. The utility crews can be expected on site within hours of the event.

Once the event has been stabilized, the surrounding facilities will require their own response, assessment, and other specialized personnel to enter the area. These businesses may have critical operations or materials that require monitoring and onsite personnel who may need relief. Controlling access to these facilities through one or two access perimeters will be challenging given the personnel are not traditional emergency responders, but fulfilling a role critical to the overall economic health of the community.

Access Challenges:

1. The utility crews and subcontracts, although not local ER personnel, will need approval to gain access to the restricted area. These personnel can be pre-enrolled in the local access program, selected by the utility, and approved for access. Some individuals may require just-in-time enrollment, approval, and delivery of the tier access tokens.

2. The density of the urban environment will compress the distances and transit times between zones, creating both potential for gridlock and congestion. The ability for the access control areas to be quickly established and communicated will facilitate smoother transit to and from the zones.

3. The challenge of managing and tracking response and recovery personnel is increased by the complex nature of the overall event. Personnel needed to conduct initial damage assessments will require access (e.g. structural engineers to inspect buildings; communication/IT engineers to restore/repair communications). The personnel, organizations, and potential suppliers who support these functions may not be ‘known’ to the local access program ahead of time and may require just-in-time access.

4. In all response and recovery activities, the logistical movement of equipment and supplies is a critical success factor. Transportation personnel (i.e. trucking) may well not be known ahead of time to the local authorities. Providing reliable access mechanisms for these personnel (and their resources) is crucial.

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

- The local access program manager should engage local CI stakeholders to discuss potential response scenarios and access requirements. This preparation enables the jurisdiction to ‘activate’ its access program and establish geographic boundaries quickly.
- The local access program manager should engage local business, CI facilities, and other organizations throughout the jurisdiction to encourage pre-registration and enrollment of personnel who may require access during an event.
- The local access program establishes a mass communication approach for response and recovery personnel, as well as local residents and non-essential workers. Keeping non-
approved personnel away from the event scene is as critical as facilitating access of approved personnel.

- Establish an interoperable access program framework to enable response and recovery personnel from outside the jurisdiction to quickly gain approval to enter.
- Provide mechanisms for just-in-time enrollment and additional access enrollment by previously registered organizations.

Summary: Urban events amplify many of the issues surrounding crisis event response. The sheer density of the environment and need to facilitate evacuation, securing the scene, and setting restricted areas will stress the local program and personnel. Crisis event response and recovery is dynamic. Pre-planning and preparation provide solid processes and coordination capabilities, but the actual execution of response and recovery activities will present unforeseen challenges. The objective of the access program should be to provide mechanisms to react to any scenario through tools and coordination amongst the parties.

Use Case 3: Impact to Community Healthcare Resources

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

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

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

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

Operational Challenges:

1. Maintaining operations before, during, and after crisis events may require additional personnel from existing hospital staff or augmentation from other medical facilities. These individuals will be going towards or into a restricted area to perform critical activities, but may not meet the expected definition of an emergency response individual.
Hospitals operate with full or nearly full staffs, which provide many support and administrative roles outside of traditional emergency responder definitions. Ensuring the availability of these staff members is critical to maintaining operations.

Hospital and State ESF-8 plans often include the steps to identify qualified and licensed augmentation staff (e.g. doctors, nurses, specialized healthcare providers, ambulatory care, etc.) to provide support to medical facilities during events. These personnel may be identified after the event and travel to the facility via their personal vehicle (POV). Ensuring these ‘authorized’ personnel have access is critical to maintaining operations.

Hospitals require near continuous receipt of supplies during events to support the increase operating tempos and workloads. This requires the expedited entry of logistical resources and healthcare related service providers.

Access Challenges:

1. Ensuring access coordination across all elements of the community’s healthcare system and support structure is key to maintaining hospital operations and providing for other community healthcare needs.
2. Ensuring the access of key personnel to maintain required staffing levels for hospitals and other essential healthcare facilities (e.g. dialysis centers) requires close integration with the local access program.
3. Providing access tokens to approved augmentation personnel, who may not be pre-registered or known to the access program.
4. Ensuring the ability to identify and support access of critical healthcare suppliers.

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

• Hospitals, along with all the other elements of a community’s healthcare support structure, form a key lynchpin in the overall healthcare resilience posture for a community or state. Engaging at both the local and state level to incorporate a consistent and interoperable approach to support access requirements for hospitals is a recommended best practice.

• Access program managers, should work jointly with their local hospitals, state health and public healthcare, and ESF-8 organizations, and appropriate licensing boards to establish a coordinated response process to ensure that augmentation personnel can be quickly identified, authorized, and delivered access tokens to expedited their transit and arrival to designated facilities.

• Hospital suppliers serve multiple communities across the country and may often re-route deliveries to impacted areas to shorten the response time. The capability of local communities to react and approve access with a consistent and interoperable approach facilitates their support.

Summary: The healthcare pyramid within the United States is ‘anchored’ by the hospital unit within a community. The ability to maintain hospital operations during and after a crisis event is critical for a community to successfully react and recover. Tight integration with the access program is a key requirement.
## Appendix B: Tier Access Definition (Draft)\(^8\)

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

\(^8\) 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

\(^9\) Used with permission. See Note 1.
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.
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.
In some cases, communications infrastructure owner/operators subcontractors require access to provide vital services such as generator management, refueling, and roof repair. These subcontractors should be afforded the same access courtesies as the communications entity they are supporting.
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

- 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
- 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/
- North Carolina Disaster Re-entry Certification Program –
- 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

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:\textsuperscript{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:\textsuperscript{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:\textsuperscript{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)\textsuperscript{14}, may be based upon required attributes, to include:

- Identification\textsuperscript{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\textsuperscript{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.
  - 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.

\textsuperscript{10} NIMS Guideline for the Credentialing of Personnel, August 2011.
\textsuperscript{11} FEMA Planning Considerations for Access and Re-entry, 2017.
\textsuperscript{12} NIMS Guideline for the Credentialing of Personnel, August 2011.
\textsuperscript{13} NIMS Guideline for the Credentialing of Personnel, August 2011.
\textsuperscript{14} NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014.
\textsuperscript{15} NIST IR 7298 Revision 2, Glossary of Key Information Security Terms, May 2013.
\textsuperscript{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.
**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.