Crisis Event Response and Recovery Access (CERRA)

Standard Operating Procedure (SOP)

Table of Contents

Acknowledgements

The authors would like to acknowledge the support and assistance of countless organizations and individuals in maturing the Crisis Event Response and Recovery Access (CERRA) programs to the point that this generalized SOP could be developed and documented.

CERRA Governance Board
CERRA Clearing House
DHS/ESSCC CERRA Working Group
Emergency Services Sector Coordinating Council (ESSSC)
State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)
Cross-Sector Coordinating Council (CSCC)
US Department of Homeland Security/Infrastructure Protection/Emergency Services
National Infrastructure Protection Plan Security & Resiliency Challenge (NIPP Challenge)
National Institute for Hometown Security (NIHS)
Pegasus Research Foundation (PRF)
National Sheriff's Association (NSA)
Mississippi Emergency Access Program (MEAP)
Mississippi Emergency Management Agency (MEMA)
Mississippi Highway Patrol (MHP)
Louisiana State Credentialing Access Program (LASCAP)
Louisiana State Police (LSP)
Louisiana Sheriff's Association (LSA)
Harris County Texas Emergency Management (HCOHSEM)
Virginia Department of Emergency Management (VDEM)

Executive Summary

Since shortly after Hurricane Katrina, members of the Emergency Services Sector Coordinating Council (ESSCC), including the National Sheriff's Association, have pressed for the establishment of better mechanisms to coordinate, secure, and enable access of critical response and recovery personnel into emergency zones before, during, and after critical events. The lack of such procedures, tools, and interoperability has delayed response and recovery timelines negatively impacting communities and amplifying the economic and individual impacts.

The Crisis Event Response and Recovery Access (CERRA) effort is the evolution of those initial priorities and represents countless hours of work across all levels of government, emergency services, state and local governments, lifeline sectors, and private, non-governmental, and volunteer organizations. The goal remains simple: to enable the secure, safe, and expedited access of response and recovery assets and personnel into emergency areas to speed response and economic recovery across the nation.

The partnership of the ESSCC and the DHS Infrastructure Protection team has enabled this goal to finally be within reach. The efforts of these groups and their key personnel supported the cross-sector, cross-government, cross-jurisdictional development of the CERRA Framework and, now, this CERRA Standard Operating Procedure (CSOP) to become a reality. Our vision is to provide these assets, plus the support and availability of the CERRA Clearing House and Outreach, Education, and Support resources to allow Jurisdictions to evaluate, define, and implement their own Emergency Access CERRA Programs.

CERRA is intended to reflect a flexible approach and is expected to continue to evolve in order to support the needs of the overall community. For CERRA, the CERRA Clearing House and the CERRA National Governance Board have been established to provide coordination and standardization support across all the Jurisdictions and Stakeholders.

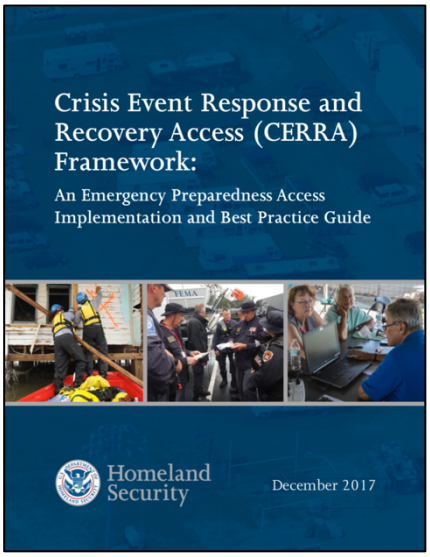
My thanks and appreciation to all parties for your continued support and input to this critical effort now and in the future.

_____

Sheriff Paul H. Fitzgerald
Sheriff, Story County, IOWA
Chairman, Emergency Services Sector Coordinating Council
Chairman, CERRA Clearing House, Inc.

1. Introduction

This document introduces, at Appendix A, a model/template CERRA Standard Operating Procedure ("CERRA SOP" or "CSOP") for emergency response and management personnel at State, Local, Tribal, or Territorial (SLTT) jurisdictions who desire to implement a phased Access Program that is consistent with the CERRA Framework[1].



1.1 Purpose

To provide jurisdictions and their stakeholders operational guidance for the implementation of a best-practices based approach to managing and implementing phased-access in support of emergency events and other activities where controlled access is required for security and safety requirements within a community.

The CERRA SOP is designed to provide guidance for those Jurisdictional personnel, who are responsible for managing and controlling access into an affected area. This CSOP extends the CERRA Framework to support the implementation elements of a successful Emergency Access Program. The CSOP includes:

- A governance process necessary to establish a successful effort,
- The steps to implement a CERRA-compliant, phased Access Program, and;
- The processes to manage the operational elements of a CERRA Access Program.

The CERRA SOP baseline template is based upon existing program documents from operational emergency Access Programs and defined to ensure operational support for Use-Cases defined by the Emergency Management, Law Enforcement, and Critical Infrastructure Sector members. As the CERRA program matures and additional jurisdictions participate in the CERRA National Governance Board[2], additional Use Cases and other resources will emerge.

1.2 Scope / Applicability

This CERRA SOP defines roles, responsibilities, and processes that should be followed during preparation, reaction, response, and recovery phases of an event to support access. The goal is to enable coordinated support to facilitate safe, secure, and effective access by critical response and recovery personnel and assets. The CSOP defines an Access Program structure that is managed and controlled at the *jurisdiction* level. Access Programs provide tools, processes, and procedures for jurisdictions to manage and control access. The scope/applicability of this CSOP is defined by the authority which implements the program.

---

[1] https://content.govdelivery.com/attachments/USDHSCIKR/2018/03/13/file_attachments/972721/CERRA%2BFramework.pdf

[2] The CERRA National Governance Board provides a governance and management process for participating jurisdictions and stakeholders to support a collaborative process for program standards, processes, and interoperability. For further information, see https://cerraaccess.org.

Participation within the overall CERRA effort and alignment with the CERRA Clearing House[3] provides the ability for programs to coordinate access across jurisdictions. The CSOP provides a set of baseline requirements consistent across all participating jurisdictions. **The CSOP provides for jurisdictions to augment these templates with local requirements as needed to implement programs in their areas.**

1.3 Administrative Provisions

The CERRA SOP is based upon a standard template managed by the CERRA National Governance Board (CNGB). By establishing a baseline template, the CERRA program provides a common reference implementation for multiple jurisdictions to utilize in establishing their own local programs and to provide a common approach that can enable interoperability across programs. Through alignment with the CERRA SOP and agreement to participate within the CERRA Clearing House, these Jurisdictional programs can leverage the software, tools, and support to establish local programs. Organizations enrolled within any participating program can be approved for access to any participating jurisdiction, thereby best supporting the ability of response and recovery organizations to support crisis event requirements on a nationwide basis.

The CNGB will, through a defined governance process, incorporate new requirements, templates, and processes into the standard CERRA SOP template on an on-going basis to support the new and evolving operational requirements of the overall CERRA stakeholders and jurisdictions. The CNGB includes representation from participating jurisdictions, law enforcement, and critical infrastructure sectors. The US Department of Homeland Security is a non-voting member of the CNGB.

Jurisdictions may also opt to implement their own local programs using components of the CERRA SOP as they see fit and not participate in the nationwide effort. Although these efforts will not have the ability to leverage the interoperability of the CERRA Clearing House and its tools and software, it is strongly believed that implementation of these best-practice processes will improve their local efforts reducing event impacts and shortening response and recovery timelines.

1.4 Oversight

The CERRA Standard Operating Procedure (CSOP) is baselined with the review, input, and concurrence of the DHS/ESSCC CERRA Working Group[4]. The document shall be controlled and

[3] The CERRA Clearing House is the public/private entity that provides interoperability between CERRA complaint access programs.

[4] Established in 2017, the joint DHS/Emergency Services Sector Coordinating Council CERRA Working Group created the initial CERRA Framework document and oversaw the establishment of the nationwide CERRA effort.

coordinated by the CNGB, an independent oversight organization led by selected members of the various stakeholders, including Emergency Services, Critical Infrastructure, and participating Jurisdictions.

2. CERRA Concept of Operations

This CERRA Standard Operating Procedure ("CERRA SOP" or "CSOP") is designed to be an operational guideline for a jurisdiction-level Emergency Access Program (EAP). This CSOP provides detailed process maps to support the multiple components, roles, and responsibilities that will be required to successfully coordinate access during a crisis event.

A CERRA program is designed to support a continuous coordination loop between the:

- Access Program Manager, nominally the Emergency Management role,
- Law Enforcement, supporting access control and checkpoint operations, and;
- Response and Recovery organizations requiring expedited access during events.

2.1 An Operational Example

The following is provided to illustrate an operational implementation of a CERRA-based Access Program. This example assumes that the program has already been established, defined, and approved. (These processes will be described within the document later.)

Preparation

Emergency Manager. As part of the establishment of the CERRA-based Emergency Access Program, the Emergency Manager has pre-defined sets of Access Level templates (rules) that can be used to support potential crisis event scenarios (Hurricane, Flood, Chemical Spill, Rail Accident, Tornado) based on the provided CERRA SOP standard templates. These Access Levels include, where applicable, specific rules that could be enforced during the identified events (e.g. HAZMAT certification during a Chemical spill/release). Through the CERRA Clearing House, a set of best practice 'Jurisdictional templates' are available to Organizations that may require access in support of response and/or recovery to that jurisdiction.

Organizations. Potential Response and Recovery organizations enroll with their local CERRA-compliant programs. Organizations may register for interest (ROI), identifying a need to maintain updated status of areas of interest. ROI is available for any participating CERRA jurisdiction.

Through the ROI process, Organizations can pre-qualify their personnel for access – by providing the specific information necessary to meet the Access Level rules established by that Jurisdiction. Through their local CERRA program and the CERRA Clearing House, Organizations manage their personnel and maintain real time knowledge of the Access approvals and status.

Law Enforcement. Law enforcement, as a full partner in the program Governance process, is entrusted with the training and tools to support activation of the Access Program, establishment of access checkpoints, and implementation of defined access levels.

Event

When an event occurs, the Emergency Manager, in coordination with other Emergency Services partners and as defined by local instruction, activates the Access Program by defining an Event.

In CERRA terminology, an EVENT is the application of one or more Access Levels (rules for entry) over a set of defined geographies over a period of time.

As an example, in the case of a flood, the EVENT may be defined by a series of restricted access zones which bounds the impacted zone along existing roadways plus some buffer. One zone may include criteria for evacuation and the most restrictive access level. Another larger area may include less restricted access to facilitate the heightened level of danger. The EVENT geography defines an emergency zone for which access is restricted. The CERRA Clearing House provides Jurisdictions with online tools which allows the EVENT and various zones to be defined via mapping tools, activated in near real-time, and communicated to stakeholders and organizations.

Through the 'activation' process:

- Law Enforcement and Organizations within the jurisdiction are notified of the EVENT and, through geolocation may be immediately available to enforce access restrictions.
- Organizations who have registered interest (ROI) are notified of the EVENT and, if applicable, make preparations to stage resources and assets for access.

Access Checkpoint/Tokens

As a component of activating the Access Program, the Access Program Manager and Law Enforcement coordinate on the establishment of Access Checkpoints, and if needed, Staging Areas. Based on the size and impact of an event, these may be coordinated with local and state Transportation personnel to support traffic routing and signage.

Organizations requiring Access utilize their local CERRA Enrollment solution, which leverages the CERRA Clearing House, to coordinate the production and delivery Access tokens (Vehicle Placards, Mobile Placards, etc.) to the Organizations and Individuals. (Note: In accordance with the jurisdiction, certain approved personnel may receive access placards at a previously defined time (e.g. resources which respond directly to emergency events have the ability to produce Vehicle Placards/Mobile Tokens at any time, including before an EVENT is activated.))

Access

Access is the process of gaining transit through, or entrance to, a restricted area or Emergency Zone. The Access tokens produced through the CERRA approach provide Law Enforcement and Checkpoint personnel with visual and electronic components to enable access control decisions.

Individuals present their access tokens to the Checkpoints and Spot Checks. Law Enforcement personnel can visually verify the tokens and authorize access *or*, using the CERRA Verify™ app, electronically validate the token and, if data communication is available, validate in real-time the approval to transit/access.

Just-in-Time/Dynamic Access

The CERRA SOP provides for mechanisms for Organizations and Access Program Managers to enable access for critical individuals not previously enrolled within a CERRA-compliant solution including mobile enrollment and mobile device distribution of access tokens.

2.2 Access Challenges

The challenge facing communities managing access during an incident are a combination of complexity and coordination. Use of a CERRA-compliant Access Program best enables jurisdictions to affect a coordinated effort across multiple response and recovery organizations and associated stakeholders to define:

- Restricted areas – WHERE access restrictions have been established to control entry;
- Access Rules – WHO, WHICH and WHEN personnel may enter; and,
- Access Authorization procedures – HOW personnel may gain access.

This CSOP provides the operational elements, processes, and components to enable these elements.

2.2.1 Phased Entry

An Access Program utilizes a Phased Entry approach, which allows for the definition of groupings, known as Access Levels, that are designed to generally correspond to the conditions within the restricted zone. During a crisis, or emergency, these might align with the level of stability and security expected within the zone in the periods following the event. When in use for crowd size events (sporting match, festival, protest, etc.) they might align with the level of security access the designated authority wants to maintain within the zone. In either scenario, the Phased Entry approach provides a mechanism for the Access Program to establish requirements which personnel and resources must meet to gain approval for access and a straightforward process to implement these restrictions. Within the Phased Entry approach, an Access Program will define specific rules to enable Access Authorization.

The CERRA Phased Entry access levels (used for crisis/emergency events) are provided in Figure 2.3.1-1.

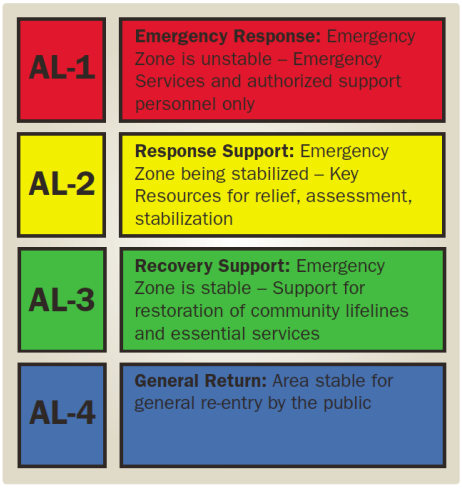


Figure 2.3.1-1: Access Level Summary

In operational terms:

- During and immediately following a tornado, the Access Program might designate Access Level-1 (AL-1) as the entry level. The impacted area condition is unknown, probably unstable, and the primary/immediate need is for trained emergency response personnel.
- As additional information is available, the Access Program might reduce the access level to AL-2 enabling key relief, damage assessment, and stabilization resources into the area. The condition may still be too dangerous (power lines down, heavily damaged structures) for repair personnel and general public, but the immediate danger is over and emergency response personnel have completed operations. (Note: Within the CERRA concepts of EVENTs, the Access Program may also change the geographic boundaries of the controlled access levels to enable areas AL-2 access while still having AL-1 in effect where Search and Rescue (SAR) operations are in effect.
- As the area becomes stabilized the Access Program would continue to lower access restrictions (AL-3) to enable access for repair and recovery assets and personnel to restart critical infrastructure and community efforts to speed the return of normal operations.

In summary, the Phased Entry approach intended to provide a flexible toolset for Access Program Managers to define access restrictions in terms of the conditions within the restricted zone, while enabling Organizations to map response and recovery resources to these conditions ensuring the right personnel can gain access at the appropriate time period.

2.2.2 Access Authorization

Access Authorization is the process and technology used within an Access Program to approve organizations (and their personnel and resources) for access at a specific Access Level.

In defining specific Access Levels, an Access Program will establish one or more rule sets, mapped to Access Levels and reflective of the potential emergency events that the jurisdiction might experience. The ‘rules’ are the logical elements organizations/individuals must satisfy in order to be approved for access.

The ‘rules’ concept employed within CERRA provides Access Programs with the capability to define (and share) those elements which organizations and individuals can provide to substantiate WHO they are, WHAT organizations they are representing, and WHAT role/skill they are providing. These are the elements by which an access decision might be made in face-to-face access decision during an event. The CERRA approach provides:

- Access Programs the ability to apply a standardized approach to access decisions,
- Organizations the capability to pre-qualify their personnel to expedite access, and;
- Law Enforcement to have vetted information available to make better access decisions.

By establishing these rule sets as part of the program, key response and recovery organizations can apply for access, provide any required information, and be ‘pre-approved’ for access prior

to any event. This status, especially if maintained within an online data system, can then be available for implementation as needed.

With the use of a CERRA-compliant enrollment solution and the CERRA Clearing House, support for just-in-time/dynamic access decisions are also available.

The CERRA approach is based on using an Attribute-based Access Control (ABAC) approach to defining Access Level rules. ABAC is a logical structure that allows for one or more independent elements (attributes or characteristics) to enable a more secure, flexible access decision. Access rules should consist of a standard set of elements to enable common widespread usage, as well as security and flexibility. These include:

Attribute	**Individual Requirement**
Identification	Possession of either: (1) Strong, secure ID credential (TWIC, CDL), *or,* (2) Federal, or State-issued government ID (Driver's License, Passport), AND, an ID issued by a known provider (employee ID, Insurance card, etc.)
Affiliation	Validation from an approved Organization (employee of, sub-contractor to, etc.)
Capability	Validation of: (1) Need to enter at specific Access Level (AL-1); *and*/*or,* (2) Specific training, certification, etc. required by the Access Level condition (i.e. HAZMAT)

Figure 2.2.2-1: General Access Rule ABAC components

Through the collection and validation in coordination with the Organization, the Access Program can establish a high degree of confidence in the decision to approve access while minimizing the collection of personnel identifiable information (PII) within the program itself.

The CERRA SOP provides detailed recommendations on standard Access Level rule sets, based both on lessons learned with existing programs, as well as, to facilitate the interoperability of programs across jurisdictions.

Within the process of defining an Access Program, the CERRA SOP provides a suite of standard Access Level definitions, rule sets and templates based on existing programs and operational experience. Each jurisdiction may need to define additional templates based on specific scenarios unique to their environments. One goal in defining the program is to use the experience and knowledge of all the stakeholders to predict, prepare, and establish the access rules for those events likely to impact the communities. The CERRA SOP is designed to enable Access Programs to add and modify Access Level templates to best meet their operational needs. When fully integrated within the nationwide CERRA Clearing House, these dynamic updates may be available across all program members to best enable response and recovery support from across the nation.

The CERRA program is coordinated at a nationwide basis via the CERRA National Governance Board (CNGB). The CNGB maintains a common CERRA SOP and provides any participating jurisdiction with all standard Access Level templates compiled from all programs to facilitate on-going lessons learned and best practices.

2.2.3 CERRA EVENTS

The EVENT concept provides a coordinated - mechanism for Access Programs to implement and coordinate access restrictions in real-time across all stakeholders.

An EVENT is the implementation of:

- An Access Level (e.g. AL-1)
- Over a defined geography
- Over a period of time.

Through EVENTS, the Access Program can specify Access requirements, the Access level rules, communicate in general terms the condition of the impacted area, communicate geographic boundaries to facilitate evacuation and the implementation of access checkpoints, and convey time period expectations.

Operationally, the Access Program Manager can pre-define a set of standard events (as preparation to potential predictable scenarios) and implement dynamically in response to real-world activities. The Access Program Manager would only need to define the geographic boundaries and start time to activate.

Within CERRA, the EVENT concept provides a real-time mechanism, via the CERRA Clearing House, to connect EVENT updates/changes to all parties who have an identified need to know, via the Registration of Interest (ROI) process. EVENT activation, geographic definition/updates, period definition/changes would all be communicated to ensure real-time coordination for organizations provided response and recovery assets and personnel.

2.3 CERRA Access Program Roles and Responsibilities

As outlined previously an Emergency Access Program (EAP) is defined by three main roles:

- Access Program Manager, nominally the Emergency Management role,
- Law Enforcement, supporting access control and checkpoint operations, and;
- Response and Recovery organizations requiring expedited access during events.

2.3.1 Access Program Manager (Emergency Manager (EM) role)

The EM's role is to manage and coordinate the response and recovery elements required for emergency events within the jurisdiction. Within the EAP this includes the preparation steps of

defining access levels, approving organizations for entry, and pre-staging EVENT templates for activation as needed. It is the responsibility of the EM to ensure that this information is communicated to all parties. This ensures that the EM manage and coordinate the access state for emergency event including the level of access and response required during each phase of response and recovery effort.

The Access Program Manager is designated as part of the Jurisdictional CERRA Standard Operating Procedure. (CSOP)

2.3.2 Access Control (Law Enforcement Officers (LEO) role)

The LEO role within an EAP is to manage the points of access (E.g. Checkpoints, Spot Checks) to facilitate assets and personnel entering or exiting the restricted area. The LEO responsibility includes responsibility for training and coordination for any personnel controlling access to the restricted zone, including review and evaluation of access placards. The LEO role works in coordination with the Access Program Manager to maintain cognizance of the access levels and defined restricted zones (geographies) and ensure communication and coordination to all checkpoint personnel. In most Jurisdictions the LEO organizations are full partners with the EM in determining how best to establish, manage, and maintain access control points and the overall security within an impacted zone.

Within the CERRA approach, Access Programs maintain this coordination via real-time updates to LEO elements via the CERRA mobile application.

2.3.3 Response and Recovery Organizations

Response and Recovery Organizations are the entities that may require access to an emergency zone to support the economic recovery of the affected region. Through coordination with the Access Program, these organizations are responsible to ensure that the individuals requiring access have met appropriate identification, membership/affiliation, role, and qualifications requirements defined by the local access rules.

Response and Recovery Organizations generally fall into four (4) categories:

(1) Local organizations – These organization are based within, or near to, the jurisdiction, and have local facilities, personnel, and/or assets. Local organizations will be known to the local Access Program Manager and participation, through the local enrollment process to ensure the timely access of personnel back into the area.

(2) Regional/National Organizations – These organizations may have local facilities, personnel, and assets, but operationally provide support to response and recovery efforts through personnel based outside of the jurisdiction. (e.g. Home Depot, Walmart) These organizations are known to the Access Program Manager, but the individuals requesting access will be identified and dispatched, often in real-time throughout the event. Registration in any CERRA-compliant Enrollment program enables issuance of

access tokens and timely access into the area. [Note: 80% of the personnel supporting response and recovery to an event will come from (2), (3), and (4).]

(3) Response Organizations – These organizations represent emergency services (and emergency support) organizations dispatched to the affected area (usually with agreement of the local authority) to provide augmentation support to the impacted emergency services. Participation in the Access Program is to support ensuring access for individuals when *not* traveling in uniform or marked vehicle (e.g. volunteer fire personnel). Per CERRA program guidelines, these organizations may register within any CERRA-compliant enroll program at no cost.

(4) Response and Recovery Support Organizations – These organizations do not have local facilities, personnel, or assets, but operationally provide support to communities through pre-existing, or just-in-time, contractual relationships. These organizations may be known to the Access Program Manager but are approved for entry when a valid reason for support is demonstrated. They will register with local CERRA-compliant enrollment providers and request access as needed through the CERRA Clearing House. With approval of the local Access Program Manager, access will be approved, and access tokens will be available for distribution and usage.

An overall objective of the CERRA coordinated approach is to enable all organizations to receive expedited access into emergency zones as necessary. This is accomplished through the coordination of jurisdictions participating via the CERRA Clearing House and Organizations registering via CERRA-compliant enrollment programs.

Organizations utilize their local enrollment programs to manage individuals and coordinate access with any participating jurisdiction via the CERRA Clearing House. The CERRA Clearing House exchanges information with the local enrollment program to determine access approval and generate and distribute access tokens as requested.

3. Development of a CERRA Standard Operating Procedure (CSOP)

Section 2 is provided as an integrated component with Appendix A: CSOP Template. These sections are the recommended baseline for any Jurisdictional CERRA EAP Program. In addition to the 'boilerplate' text, the sections below include questions Jurisdictions will need to address to finalize their CSOP.

This CERRA Standard Operating Procedure must be utilized along with the CERRA Clearing House (https://cerraaccess.org) in order to create CERRA Access Credentials and receive nationwide interoperability.

3.1 Overview

This Crisis Event Response and Recovery (CERRA) Access Program Standard Operating Procedure (SOP) is required in order to assist in the definition, implementation, and maintenance of an Access Program for the jurisdiction. This operating procedure is intended to create an Emergency Access Program that both services the access and reentry needs of the jurisdiction, while also allow for interoperability between other CERRA participating jurisdictions.

The structure of this document will allow the jurisdiction to have the operating procedure necessary to implement an Access Program. This operating procedure, when combined with the CERRA Clearing House, allows the jurisdiction Access Program to become fully interoperable with all other CERRA programs nationwide.

The sections below outline the basic operational procedure of this Access Program. These sections will offer flexibility to address both standard emergency events, as well as, any unique event cases identified for the jurisdiction. This jurisdiction CSOP will be reviewed and updated as necessary, but not less than annually.

Q: What jurisdiction does this Standard Operating Procedure apply to?
Q: Will this Standard Operating Procedure incorporate other localities in your region, county, city, etc.?

3.2 Definition of Authority

This Jurisdictional Access Program is implemented under legal authority designed by local and/or state law or instruction.

The Access Program Manager for this Jurisdiction Emergency Access Program is designated as the Emergency Manager.

An Access Program must also have a designated Access Program Manager. This person's responsibilities are to coordinate the activation of the Access Program, coordinate the Access

Program implementation, and manage the Access Program's response during an event. All of these responsibilities are expected to be done in a coordinated fashion, with the Access Program Manager's role being augmented by additional support staff.

Note: Emergency Access Programs operate under legal authority of the local and/or state jurisdiction(s). For operational clarity, and to be consistent with the National Incident Management System (NIMS), the CSOP requires the designation of a primary lead. Larger jurisdictions may identify multiple leadership positions, but the Access Program Manager is the primary coordinator for the program.

An Emergency Access Program is "activated" in order to be utilized by all stakeholders. This action is carried out by the legal authority authorized for the Jurisdiction. This "activation" is the formal direction that the program will be utilized for a specific time frame (EVENT) or for a specified duration (year, month, etc.)

In order to activate the Access Program according to this CERRA Standard Operating Procedure, there may need to be a formal declaration of a state of emergency either by the local/statewide Emergency Manager or by a local/statewide elected official. (Note: The pre-requisites of "Activation" should be determined with the local authority and documented in this CSOP. The required process varies according to state and local law.) An emergency declaration will result in a communication by various parties including Access Program representatives notifying all stakeholders that a form of Access (reentry, commercial event, etc.) will be initiated.

Q: Who is the Access Program Manager for this Standard Operating Procedure?
Q: What organization does the Access Program Manager represent?
Q: What gives the Access Program Manager the authority to operate this Access Program (procedure, role, law, etc.)?
Q: What other actions/processes (e.g. Directive/Declaration by elected official) must be executed (prerequisites) for program activation?

3.3 Establishment of Governance Board Process

An Access Program is a cross-jurisdictional, cross-sector, cross-government effort. Successful implementation requires the active and engaged participation of stakeholders within a local jurisdiction. A Governance Board is the coordination of these stakeholders. It is designed to provide mechanisms to ensure the Access Program is best serving the needs of the jurisdiction and its communities.

Governance Board processes will vary in size and make-up based on the local jurisdiction, the structure of the government, and the critical infrastructure sectors that form the backbone of the local communities. The governance board can be comprised of a formal collection of representatives from a jurisdiction or an added responsibility for previously established groups (e.g. Local Emergency Planning Committee).

The Governance Board responsibilities are:

(1) To establish a collaborative environment to develop, review, and approve the initial CERRA SOP for program implementation,
(2) Maintain on-going review, coordination, and cooperation via regular meetings.
(3) To establish a forum for which stakeholders can raise issues and new requirements that may need incorporation into the SOP for best implementation of the program.

Governance Boards should include sufficient membership to ensure representation of all key government entities, including state or regional authorities (if implementation of the program requires their support and/or coordination), but limited to be an effective body. The Access Program Manager, designated under the Authority section, should define a small group representing the key Emergency Management, Law Enforcement, and Critical Infrastructure representation to lead the Governance Board.

The primary goal of the Governance Board is the definition and maintenance of the jurisdiction's SOP. Development of organization specific instructions and/or general orders should remain the responsibility of the various organizations.

For the jurisdiction, the program Governance Board will consist of:
[List by roles/positions & names]

Q: What organizations or agencies will be represented on the Governance Board?
Q: How regularly will the Governance Board meet?

3.4 Roles and Responsibilities

In support of implementation of an Access Program, the following section will assist in defining the roles and responsibilities of the various coordinating parties within a jurisdiction. The Governance Board can also publish specific direction on these roles and responsibilities in order to further define any specific areas.

The CERRA approach defines a set of 'roles' to best coordinate the Access Program support components:

- Definition and Coordination of Access
- Access Control
- Implementation (Activation) of Access

In this Standard Operating Procedure, these roles will be defined in the following context:

- Access Program Manager (Definition/Coordination of Access)
- Law Enforcement (Access Control)
- Response and Recovery Organizations (Implementation of Access)

A more detailed outline of the roles and responsibilities for these elements is provided below:

3.4.1 Access Program Manager (nominally the Emergency Manager)

The Access Program Manager for the Jurisdiction Access Program is: John Doe

The Access Program Manager's role is to manage and coordinate the response and recovery elements required for emergency events within the jurisdiction. Within this Access Program this role includes the preparation steps of defining access levels, approving organizations for entry, and pre-staging EVENT templates for activation as needed. It is the responsibility of the Access Program Manager to ensure that this information is communicated to all parties. This ensures that the Access Program Manager is able to manage and coordinate the access state for emergency events, including the level of access and response required during each phase of response and recovery effort.

Q: Are there any additional roles the Access Program Manager needs to fill that are specific to your jurisdiction?

3.4.2 Access Control (Law Enforcement Officers)

The Access Control role for this jurisdiction will be fulfilled by the following agencies:
Local Police Department
State Department of Public Safety (Highway Patrol)

The Access Control role within an Access Program is to manage the points of access (i.e. Checkpoints, Spot Checks) and to facilitate the assets and personnel entering or exiting a secure/restricted area. The Access Control responsibility includes responsibility for training and coordination for any personnel controlling access to the restricted zone, including review and evaluation of access placards. The Access Control role works in coordination with the Access Program Manager to maintain cognizance of the access levels, defined restricted zones (geographies), and to ensure communication/coordination with all checkpoint personnel.

Within the CERRA approach, the Access Control Leads and Access Program Manager communicate and coordinate throughout the process via established procedures and the Emergency Operations Center (EOC). The CERRA Clearing House provides mobile applications that allows real-time coordinate across these vital roles. These applications are offered to jurisdictions to support seamless coordination and communication during activation.

The Access Control role in this Standard Operating Procedure is designated as the local law enforcement entity, with augmented support by requested state law enforcement (Department of Public Safety) resources.

Q: What law enforcement agencies will be fulfilling this role in your jurisdiction (Sheriff, PD, State DPS, etc.)? Please list multiple if applicable.

Q: How do the law enforcement organizations provide coordinated support during emergencies? (ESF-13 Desk?)

3.4.3 Response and Recovery Organizations

Response and Recovery Organizations are the entities that may require access to an emergency zone to support the economic recovery of the affected region. These organizations include both stakeholders in a local jurisdiction, out of jurisdiction supporting entities, and all applicable Critical Infrastructure (CI) and Business sectors. Through coordination with the Access Program, these organizations are responsible to ensure that the individuals requiring access have met appropriate identification, membership/affiliation, role, and qualifications requirements defined by the local access rules. These requirements are set based off of the event and response/recovery needs at a specific time.

All organizations in the categories listed below are approved by the Access Program Manager for access into a jurisdiction. These organizations can be identified at a checkpoint or access entry location by a preapproved CERRA access credential or, in certain situations, vehicle markings/predefined identification issued by the local jurisdiction.

Response and Recovery Organizations fall into four (4) categories:

(1) Local Organizations – These organization are based within, or near to, the jurisdiction, and have local facilities, personnel, and/or assets. Local organizations will be known to the local Access Program Manager and participation, through the local enrollment process to ensure the timely access of personnel back into the area. Organizations in this category are required to register for CERRA access credentials with the Access Program.

(2) Regional/National Organizations – These organizations may have local facilities, personnel, and assets, but operationally provide support to response and recovery efforts through personnel based outside of the jurisdiction (e.g. Chevron, Walmart). Organizations in this category will comprise various sectors but traditionally be private and responding in order to recover and restart their facility operations. These organizations are known to the Access Program Manager, but the individuals requesting access will be identified and dispatched, often in real-time throughout the event. Organizations in this category are required to register for CERRA access credentials with the Access Program and eligible for nationwide CERRA interoperable access credentials.

(3) Response Organizations – These organizations represent emergency services (and emergency support) organizations dispatched to the affected area (usually with agreement of the local authority) to provide augmentation support to the impacted emergency services. Organizations falling under this designation may be both public and private but generally respond in a life-saving or essential services capacity. Organizations in this category may register for CERRA access credentials into the Access Program or be identified by marked vehicles and/or previous local instruction.

(4) Response and Recovery Support Organizations – These organizations do not have local facilities, personnel, or assets, but operationally provide support to communities through pre-existing, or just-in-time, contractual relationships. These organizations may be known to the Access Program Manager and are approved for entry when a valid reason for support is demonstrated. These include private organizations both contracted by a local jurisdiction and those that are supporting other resources. Organizations in this category are required to register for CERRA access credentials with the Access Program and eligible for nationwide CERRA interoperable access credentials.

The overall objective of the CERRA coordinated approach is to enable all organizations to receive expedited access into emergency zones as necessary. Organizations that register for CERRA access credentials are utilizing the CERRA Clearing House and a regional CERRA provider to ensure expedited access into the local jurisdiction. These organizations may also request access to other jurisdictions throughout the nation, and those access decisions have no effect on the access decision made by the local jurisdiction or Access Program Manager.

Organizations will utilize a local CERRA provider in coordination with the CERRA Clearing House to manage individuals and coordinate access with any participating jurisdiction. The CERRA Clearing House exchanges information with CERRA service providers to determine access approval and generate and distribute access credentials as requested.

Q: The Access Program should consider the inclusion of 'Lifeline' Response and Recovery organizations within the Access Program process, including the Governance Board. Based on your Jurisdiction and the potential scenarios are their Organizations that should be included?

3.4.4 Use Cases/Access Requirements

The objective of an Access Program is to facilitate the expedited access of critical response and recovery assets to enable safer, more secure, and more effective return to normalcy for the community. This is both a security priority and an economic imperative. The section below includes template Use Cases as well as unique Access Requirements for this jurisdiction.

Use Cases

This CERRA Standard Operating Procedure includes two predefined Use Cases, or access templates, and will be utilize for potential events. This Use Cases are intended to be generic for their broad application to multiple potential events under the same event category. All information not outlined in the below Use Cases, is considered to operate the same as Standard Operating Procedure or is defined within the CERRA Online Application in conjunction with the CERRA Clearing House and a local CERRA provider.

Hurricane Use Case (Access Template Example)

EVENT Designation: Hurricane “Name”

Activation Requirement: State of Emergency Declared by State Authority

Geographic Activation Area: Multi-Jurisdictional

Access Program Manager: Local Jurisdiction Emergency Manager

Access Control: Local Jurisdiction Law Enforcement

Predefined Access Control Points (Checkpoints):

- Intersection of Main Street and Johnson Street
- Andrews Street Exit (15) from Route 50
- Route 50 prior to Samuel’s Bridge

Initial Access Level: Access Level 1

Activation Communications Resources: CERRA Application, 411, Variable Message Boards, Local Radio Station, Online Media/Social Network.

Access Credentials (One is Required): CERRA Access Credential, Marked Utility Vehicle/ID, Marked Emergency Response Vehicle/ID, Local Government Employee Emergency Responder Badge.

July 4th Parade Use Case (Access Template Example)

EVENT Designation: July 4th Parade

Activation Requirement: Access Program Manager’s Request

Geographic Activation Area: Main Street

Access Program Manager: Local Jurisdiction Emergency Manager

Access Control: Local Jurisdiction Law Enforcement

Predefined Access Control Points (Checkpoints):

- Intersection of Main Street and Johnson Street
- Intersection of Main Street and Robinson Street
- Samuel’s Bridge inbound lanes after Route 50

Initial Access Level: Access Level 3

Activation Communications Resources: CERRA Application, Local Radio Station, Online Media/Social Network.

Access Credentials (One is Required): CERRA Access Credential, Marked Utility Vehicle/ID, Marked Emergency Response Vehicle/ID, Local Government Employee Emergency Responder Badge.

The defined templates shown above are utilized for predefined event types. These templates only represent a small portion of potential events to affect a jurisdiction but offer an opportunity to immediately implement an Access Program without any pre-coordination required. All templates may be predefined in the CERRA Application for easy access and activation.

Q: What are the 'likely' events that your jurisdiction has established due to geography, past experience, etc.?
Q: What predefined templates would your jurisdiction like to incorporate into this Standard Operating Procedure? Please fill in one or more templates and use the examples as a guide.

Access Requirements

This Standard Operating Procedure includes Access Requirements that are used to define specific rules required for receiving access into this jurisdiction. Any rules not covered below fall under the Standard Operating Procedure included in other sections.

Access Credential Requirements

In terms of Access Credentials, personnel requesting access into a secure area are separated into two groups: Emergency Responders, Response and Recovery Organization.

Emergency Responders are personnel who represent local law enforcement, local fire departments, the local/regional Utility Company, local emergency response designated government employees, and all other organizations that fall under the Emergency Services Sector. These organizations are able to identify themselves at an Access Point (Checkpoint) by using **one** the following means:

- Marked Vehicles
    - Local/Regional Emergency Responders must have their agency's name clearly marked on their vehicle with additional identification available if requested.
    - The Local/Regional Utility Company falls into this category, any vendor/contractors must either come in a Utility Company marked vehicle or register for a CERRA Access Credential.
- Emergency Responder ID

- Local government employees designated as “Emergency Responders” on their jurisdiction issued ID badge, may present this badge at checkpoints for access into a secure area.

- CERRA Access Credential
  - All above organizations can register for an Access Level 1 CERRA Access Credential to be preapproved to receive access into a secure area within the jurisdiction.
  - The CERRA Access Credential is provided by the local CERRA provider. Please refer to https://sample.com for more information.

Note: All organizations in the above category fall under Access Level 1.

Response and Recovery Organizations are personnel who represent Critical Infrastructure, local businesses, regional/national organizations, and all other applicable commercial and/or public sectors. These organizations identify themselves at a checkpoint through the following means:

- CERRA Access Credential
  - All above organizations can register for an Access Level 1, 2, 3, or 4 CERRA Access Credential to be preapproved to receive access into a secure area within the jurisdiction.
  - Personnel receiving a CERRA Access Credential are required to carry one form of Government Identification with them to receive access.
  - The CERRA Access Credential is provided by the local CERRA provider(s). Please refer to https://sample.com for more information.

Note: The Access Control role (Law Enforcement) maintains the access decision at the checkpoint and can request additional documentation or additional identification as necessary.

Additional access requirements may be added to specific events within the jurisdiction at a later date. These access requirements may require additional training (ex. HAZMAT Certified) or a restriction on access to certain areas (ex. Military Base).

Q: What unique Access Requirements need to be added for your jurisdiction? (These requirements allow organizations to receive access without a credential, ensure any added requirements are secure and easy for all law enforcement to identify).
Q: What is the primary “Utility Company” for your jurisdiction? Would you like to identify them by name, or identify them as “Electric Power Companies” for a general representation? Please fill in the appropriate information.

3.4.5 Access Program Management Role

An Access Program is operated under the Definition of Authority. An organization (or individual) is designated as the Access Program Manager.

The Access Program Manager is responsible for the implementation and operations of the program. The Access Program Manager operates the program in accordance with the SOP defined and approved by the Governance Board.

The Governance Board provides oversight and coordination support for the Access Program.

3.5.6 Access Program Training, Coordination, Implementation

Access Program Training, Coordination and Implementation is the responsibility of each of the stakeholder organizations. The CERRA National Governance Board and CERRA Clearing House provide support, tools, and technology to organize, implement, and operate the local Access Program(s). Participation by Response and Recovery organizations is coordinated by the local CERRA provider(s) selected by the jurisdiction. The CERRA Clearing House works in conjunction with the local enrollment provider(s), requiring their compliance with the CERRA technical interfaces necessary to support implementation of the jurisdictional defined EVENTS, Access Levels, and CERRA Access Credentials.

Q: Do you want to list any specific training requirements or training schedules in this section? (i.e. Training materials will be distributed to all law enforcement at the start of Hurricane Season)

3.5.7 Access Program Activation

The Access Program is 'activated' for usage by processes defined within the CSOP instruction and the Definition of Authority. The Access Program Manager, upon activation, enables coordinated response and recovery with all registered stakeholders.

3.6 Access Levels

The Access Program utilizes a Phased Entry approach, which allows for the definition of groupings, known as Access Levels, that are designed to generally correspond to the conditions within the restricted zone. During a crisis, or emergency, these might align with the level of stability and security expected within the zone in the periods following the event. When in use for crowd size events (sporting match, festival, protest, etc.), they might align with the level of security access the designated authority wants to maintain within the zone. In either scenario, the Phased Entry approach provides a mechanism for the Access Program to establish requirements which personnel and resources must meet to gain approval for access and a straightforward process to implement these restrictions. Within the Phased Entry approach, the Access Program defines specific rules to enable Access Authorization.

Figure 2.3.1-1 © Pegasus Research Foundation 2018

The CERRA Phased Entry access levels (used for crisis/emergency events) are provided in Figure 2.3.1-1.

The Phased Entry approach is utilized to provide a flexible toolset for Access Program Managers to define access restrictions in terms of the conditions within the restricted zone, while enabling Organizations to map response and recovery resources to these conditions ensuring the right personnel can gain access at the appropriate time period.

Q; Based on your scenarios, are their adjustments to the mapping of Access Levels (AL) to the specific capabilities needed for response & recovery? Document these to implement in your configuration.

3.6.1 Access Level Rule Elements

Access Levels are defined to enable jurisdictions to make better access decisions. The approach defines a set of required identity attributes that, when validated, verified, or vouched, enable the automated satisfaction of the rules defined within the program and the immediate approval of access and access tokens.

This CERRA Standard Operating Procedure leverages the CERRA approach and existing CERRA Access Programs to define standardized Access Level rules. The table below and Appendix A provide detailed information on the Access Level standard rules.

Access Level	Attribute Element	Description/Requirement	(M) / (O)*
AL-1	Identification	Valid Government-issued Photo-ID Valid Access Level 1 CERRA Access Credential Valid Organization Issued Badge Marked Emergency Response Vehicle Marked Utility Company Vehicle Local Government Emergency Responder Badge	M M O O O O
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-1 Response/Recovery personnel	M
AL-2	Identification	Valid Government-issued Photo-ID Valid Access Level 2 CERRA Access Credential Valid Organization Issued Badge	M M O
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-2 Response/Recovery personnel	M
AL-3	Identification	Valid Government-issued Photo-ID Valid Access Level 3 CERRA Access Credential Valid Organization Issued Badge	M M O
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-3 Response/Recovery personnel	M
AL-4	Identification	Valid Government-issued Photo-ID Valid Access Level 4 CERRA Access Credential	M M
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-4 Response/Recovery personnel	M

***Mandatory (M)/ Optional (O)**

Q: Do you need to add any additional requirements to the above listed Access Levels? (reference Appendix A section 3.4.4. for any new access requirements).

Identification
Organizations and personnel responding during an event must present the mandatory identifications required at a checkpoint into a secure area. The mandatory identifications listed above are those that the Access Control role (Law Enforcement) are trained to identify a checkpoint. These credentials may be verified by either visual inspection, a mobile/desktop application, or a direct support line.

The Access Control role may request both mandatory and optional credentials at a checkpoint, and the standing recommendation will be to bring all possible forms of identification within a desired Access Level when responding to an event.

Please refer to Appendix A and Access Requirements in Appendix A section 3.4.4. for further information on required formats or additional access requirements.

Membership/Affiliation
All personnel that request access within the Access Program will be required to be a member of or have an affiliation with a responding organization. The organization must vouch for all personnel that are designated for response purposes, and those personnel must bring their approved access identification to demonstrate their membership/affiliation.

The CERRA Approach, in conjunction with the CERRA Clearing House and local CERRA provider(s), gives organizations the ability to vouch for personnel and allow their personnel to create CERRA Access Credentials to demonstrate a membership/affiliation. Organizations must register and vouch for their personnel through CERRA, unless they meet one of the other listed Access Requirements in Appendix A section 3.4.4.

Roles/Capabilities
Organizations will assign specific roles and capabilities to their personnel when responding to an event. These roles/capabilities are designed to inform both the Access Program Manager and Access Control of their purpose for responding to the local jurisdiction.

The Access Program Manager will be given all assigned roles/capabilities of personnel within a jurisdiction to assist in informing access decisions. The CERRA application will be used by the Access Program Manager to utilize a jurisdiction specific dashboard in order to manage these roles/capabilities in an expedited manner.

Permission
Permission is the approval of the Organization for a specific employee (or contractor) to respond to an EVENT. Many personnel **may** meet the Access Level requirements established by

the Jurisdiction for an EVENT, but the Organization will only designate (approve) those individuals necessary to affect the required response and/or recovery mission. The concept of permission ensures that (a) only those individuals required by the Organization respond, limiting the risk to its employees and business and (b) that the Organization respects the direction of the Jurisdiction by only having required resources active during the EVENT.

Access Level Definition

The Access Levels for this CERRA Standard Operating Procedure are defined in the below table. These definitions outline the organizations expected to respond during an event, and the Access Level that they will be designated. These Access Level definitions are subject to change based on the event, and organizations may have personnel in their organizations who receive different Access Level approvals based off of their designated role/capabilities.

The Phased Access process for this Standard Operating Procedure follows the standard CERRA guidelines. Please refer to figure 2.3.1-1 for general access level references.

Access Level	Description/Requirement
Access Level 1 – Emergency Response (RED)	Emergency Responders • Fire Departments • EMS • Local, State, Federal Law Enforcement • Search & Rescue • Local Jurisdiction Designated Emergency Response Personnel Military (Including National Guard and Coast Guard) Designated Regional Utility Company Essential Medical Personnel (ESF-8) Critical Infrastructure/Key Resource Essential Response Teams Critical Infrastructure Lifeline Sector Essential Response Teams Other personnel at the approval of the jurisdiction
AL-2 – Response Support (YELLOW)	Critical Infrastructure/Key Resource Response Support Personnel • Vendor/Contractor Organizations of Response Support Personnel • Damage Assessment Teams Critical Infrastructure Lifeline Sector Response Support Personnel • Damage Assessment Teams Security Organizations Official Damage Assessment Teams (FEMA, State, Local) Private/Public Sector Organizations Response and Damage Assessment Teams Voluntary Organizations Active in Disaster (VOAD) Response Teams Insurance Provider Damage Assessment Teams Other personnel at the approval of the jurisdiction
=AL-3 – Recovery Support (GREEN)	Critical Infrastructure/Key Resource Recovery Personnel • Vendor/Contractor Organizations Critical Infrastructure Lifeline Sector Recovery Personnel Private/Public Sector Organizations Recovery Personnel Voluntary Organizations Active in Disaster (VOAD) Recovery Teams Other personnel at the approval of the jurisdiction
AL-4 – General Return (BLUE)	General population return Other personnel at the approval of the jurisdiction

Q: Are there any additional organizations you want to explicitly identify in the above table? (This may be valuable for key organizations or industries)

3.6.2 Access Approval

Access Approval and preapproval into a jurisdiction will be decided by the Access Program Manager. All Access Approval request must be decided by the jurisdiction prior to an organization or their personnel receiving entry into a secure area. These approvals will allow the organization to produce CERRA Access Credentials or receive access via the other established access requirements.

The Access Program Manager can utilize the CERRA Application as well as predefined access best practices to expedite the jurisdiction access approval decisions.

Access Control personnel (Law Enforcement) will retain the final decision for access at checkpoints into a secure area. These personnel can use their discretion to accept or reject pre-approved access decisions if necessary.

3.7 Preparation - Coordination

In response to a potential event there is pre-incident coordination required between the local jurisdiction, Access Control personnel, Access Program Manager, and response/recovery organizations. This process is defined below to ensure a smooth transition from pre-incident to activation.

3.7.1 Access Registration/Maintenance

- Personnel requiring access and not meeting any predefined Access Requirements must pre-register for CERRA Access Credentials to ensure they can receive access during an event or post event.
    - The CERRA Access Credential registration is made available through local CERRA provider(s) working in conjunction with the CERRA Clearing House. Please visit (https://cerraaccess.org) for more information.
- Organizations must update and perform routine maintenance on their preregistered personnel roster to ensure that all appropriate personnel are registered, affiliations/memberships are identified, and roles/capabilities are assigned.
    - **Affiliation/Membership Example:** Employee/Employer registers and vouches for their response teams to receive CERRA Access Credentials.
    - **Role/Capability Example:** An Organization identifies their personnel as a "Damage Assessment Team" and assigns that role on their CERRA Access Credential.
- Pre-Identifying essential personnel and their Access Levels.

  - Organizations must be notified of their requirement to register for CERRA Access Credentials or their ability to meet other predefined Access Requirements within the local jurisdiction.
- Preparing Vehicle Placards, Letters of Access (LOA), or Mobile Placards for essential personnel
  - The jurisdiction is required to prepare, maintain, and distribute Placards that meet the criteria defined in by the CERRA Clearing House. In order for these Placards to be CERRA compliant they must integrate with the CERRA Clearing House (https://cerraaccess.org)
  - A local CERRA provider(s) will be designated to provide these Placards, distribute them, and maintain them on a yearly basis at no-cost to the jurisdiction.

3.7.2 Access Control (Law Enforcement) Preparation

Access Control personnel (Law Enforcement) will also require coordinated pre-incident preparation to ensure they are able to establish the appropriate checkpoints and identify organizations approved for access into a jurisdiction.

The pre-incident coordination for Law Enforcement will predominantly focus on communicating predefined checkpoint locations (see: Appendix A Section 3.4.4.) and distributing training materials to ensure that the Access Requirements and Identifications are understood and able to be executed on during an event.

It is the responsibility of the local jurisdiction and Access Program Manager to assist in law enforcement training coordination for their jurisdiction. The materials for this training can be created and distributed by local CERRA provider(s) in conjunction with the CERRA Clearing House.

Q; Do you want to identify or cite any specific procedures for post-evacuation access or event access in this section? (i.e. Muster points, or specific procedure that would be relevant to access control preparation).

3.7.3 Registration of Interest (ROI)

Organizations are required to register interest for access into jurisdictions they wish to receive access to. These organizations must some their Registration of Interest to the Access Program Manager so that they can receive an access decision. Organizations can submit this registration of interest before, during, or post-event and the Access Program Manager can approve or disapprove the organization based on the information provided.

The Access Program Manager can choose to utilize the CERRA Application dashboard and local CERRA provider(s) to receive, organization, and coordinate these registrations of interest and access decisions.

3.8 Organization Registration – Enrollment Provider(s)

This Standard Operating Procedure designates CERRA Enrollment Provider(s) that can assist in the coordination of the program, registration of organizations, and outreach/training for the jurisdiction. The Enrollment Provider's responsibility is to work in conjunction with the CERRA Clearing House to ensure that the jurisdiction is provided all the necessary resources for an Access Program at no-cost, while also ensuring the jurisdiction is able to integrate nationally with the CERRA Clearing House.

The designated CERRA Enrollment Provider(s) for this jurisdiction is/are: [Insert Provider Name Here]

The CERRA Enrollment Provider(s) for the jurisdiction will handle or assist with the following responsibilities:

- Organization Registration
  - The designated CERRA Enrollment Provider will provide a platform to register organizations for access decision approvals and CERRA Access Credentials.
- CERRA Access Credential Creation/Distribution
  - The designated CERRA Enrollment provider(s) will organize, create, and offer a method of distribution for CERRA Access Credentials.
- Private/Public Sector Outreach
  - The designated CERRA Enrollment provider(s) will assist in public and private outreach campaigns, events, and other meetings to ensure the jurisdiction understands the required procedure for the Access Program.
- Law Enforcement Training
  - The designated CERRA Enrollment provider(s) will assist in distributing the materials for law enforcement training as well as offering individual sessions to assist in training throughout the year.

Q: What CERRA Provider(s) is your jurisdiction working with? (Please contact the CERRA Clearing House at https://cerraaccess.org for more information on providers)

3.9 Checkpoint Operations

Checkpoints are defined as access points utilized by law enforcement or Access Control personnel designed to control access into a secure or restricted area. In the Standard Operating Procedure Checkpoint's are operated by Access Control personnel (Law Enforcement). There are three types of operational checkpoints that may be used in order to control access into an area.

- Outer Checkpoints
  - Outer Checkpoints are access points established at the furthest point outside of a restricted or secure area to facilitate the controlled access of personnel and vehicles. These checkpoints are designed to be used for expedited access into a

secure area by quick identification of CERRA Access Credentials or other associated access points.
    - Outer Checkpoints are set with the lowest required Access Level into a jurisdiction. This is to ensure that no other Inner Checkpoints conflict with the Outer Checkpoint access level, and to allow a seamless transition between Access Levels for responding organizations.
- Inner Checkpoints
    - Inner Checkpoints are access points established within a restricted or secure area in order to further control access to the least stable areas within the jurisdiction. These checkpoints are staged in areas that require more restrictive access (higher access level) and/or are unsafe for general response personnel to enter.
    - Inner Checkpoints will always be designated at least one access level higher than the established Outer Checkpoints. These checkpoints may require a more detailed or scrutinized review of an individual's CERRA Access Credential or other Access Requirements due to the unsafe nature of the restricted area.
- Spot Checks
    - Spot Checks are access points that are implemented in a roaming capacity to ensure individuals who are within a restricted area meet the appropriate access requirements or have a CERRA Access Credential. These are designed to ensure that no unauthorized personnel are accessing restricted areas during an event.
    - Spot Checks are used to verify that an individual had the appropriate access level to pass through an Outer or Inner Checkpoint and are implemented at law enforcement's discretion or by the request of the Access Program Manager.

Q: Are there any additional checkpoints or access points you would like to identify in this section? (i.e. Unique access situations that do not fall under the above three categories).

3.10 Activation

Activation is the process of activating the Access Program in preparation for or response to an Event. The process of authority for activation is discussed in Appendix A Section 4.7, the process and steps for activating the program once authority has been given are outlined below:

1. Designating an event
    - The Access Program Manager must designate the appropriate event for activation. An event can range from an emergency situation to any type of event within a jurisdiction that would require restricted or controlled access. This event must be designated in a pre-approved format that is made visible on the CERRA Access Credentials. The jurisdiction may choose to use a CERRA compliant provider to designate the event status.
2. Approving access
    - The Access Program Manager must preapprove access for organizations requesting entry into a secure/restricted area during an event. These access decisions must be

communicated to the organization and made visible on the CERRA Access Credentials. Organizations that meet the other Access Requirements for Access Level 1 defined in Appendix A Section 5.1.5 are eligible to receive automatic preapproval. The jurisdiction may choose to use a CERRA compliant provider to organize and approve access decisions.

3. Creating and distributing access credentials
    - Access Credentials must be distributed to organizations requesting access into the jurisdiction. These credentials must meet the format outlined in Appendix A and must be distributed pre-event. The jurisdiction may choose to use a CERRA compliant provider to create and distribute these credentials.

4. Establishing checkpoints
    - The Access Control personnel (Law Enforcement) are responsible for establishing checkpoints according to Appendix A Section 8 and following any predefined Use cases outlined in Appendix A Section 4.4. The jurisdiction may choose to use the CERRA Application Dashboard to denote the checkpoint locations.

Q: Are there any communications requirements you would like to add to this section? (i.e. Variable Message Boards, 411, local News, will all receive an Activation notice).

3.10.1 Event Updates

The Access Program Manager is required to update the event status and communicate those updates to the Access Control personnel and response and recovery organizations. These updates include the following:

- Access Level Changes
- Checkpoint Location Changes
- Additional Event Restrictions (HAZMAT, etc.)
- Event Activation Status (Active, Inactive, etc.)
- Event Duration Status
- Curfew Status

All of these updates must be communicated to all applicable stakeholders within a jurisdiction to ensure seamless coordination during the reentry process. The jurisdiction may use the CERRA Application and a local CERRA provider to coordinate all of these updates.

Q: Are there any curfew procedures in your jurisdiction you would like to cite in this document?

3.10.2 Updated Access Credentials

Access Credentials must be updated to match the Event Updates or other associated criteria. Please refer to Appendix A to understand what areas must be updated when Event Updates occur within a jurisdiction.

3.10.3 Enable Just-in-Time Access

Access Credentials must be available for immediate distribution for organizations who require "Just-In-Time" access. These organizations are ones that respond immediately post-event, and do not have the ability to identify personnel or vehicles until they are dispatched for a response effort.

The Access Program Manager must either have an interface to distribute these Placards to establish defined muster points during activation where Access Credentials can be distributed to incoming personnel. The jurisdiction may utilize a CERRA enrollment provider to manage the Just-In-Time delivery of CERRA Access Credentials.

Q: Are there any muster points or areas where credentials may be distributed you would like to identify? (Note: All credentials can be distributed in a mobile format through email/text).

3.11 On Going Operation and Refinement

This Standard Operating Procedure will go through a routine update and refinement process to ensure that any new requirements, use-cases, or other stakeholder inputs are included. These 'new' requirements may be requested from the CERRA National Governance Board to maintain interoperability or may be added to support local-only jurisdictional requirements that need to be accepted in order to refine operations of the Access Program.

The on-going operation and refinement process of this operating procedure will be handled collectively by the Access Program Manager and Governance Board defined in Appendix A Sections 3.4.1 and 3.3 respectively.

Appendix A – CERRA Standard Operating Procedure (CSOP) Template

CERRA STANDARD OPERATING PROCEDURE[Jurisdiction Name]

CERRA Standard Operating Procedure (CSOP) ACTIVE [Date]
[Organization Name] | [Organization Address]

Table of Contents

1.0 Overview

This Crisis Event Response and Recovery (CERRA) Access Program Standard Operating Procedure (SOP) is required in order to assist in the definition, implementation, and maintenance of an Access Program for [jurisdiction.] This operating procedure is intended to create an Emergency Access Program that both services the access and reentry needs of the jurisdiction, while also allow for interoperability between other CERRA participating jurisdictions.

The structure of this document will allow [jurisdiction] to have the operating procedure necessary to implement an Access Program. This operating procedure, when combined with the CERRA Clearing House, allows the [jurisdiction] Access Program to become fully interoperable with all other CERRA programs nationwide.

The below sections will outline the basic operational procedure of this Access Program. These sections will offer flexibility to address both standard emergency events, as well as, any unique event cases identified for [jurisdiction.] This [jurisdiction] CSOP will be reviewed and updated as necessary, but not less than annually.

2.0 Definition of Authority

This Jurisdictional Access Program is implemented under legal authority designated by [local and/or state law or instruction.]

The Access Program Manager for this [Jurisdiction] CERRA Access Program is the person designated as [role (ex. Emergency Manager).]

An Access Program must also have a designated Access Program Manager. This person's responsibilities are to coordinate the activation of the Access Program, coordinate the Access Program implementation, and manage the Access Program's response during an event. All of these responsibilities are expected to be done in a coordinated fashion, with the Access Program Manager's role being augmented by additional support staff.

Note: Emergency Access Programs operate under legal authority of the local and/or state jurisdiction(s). For operational clarity, and to be consistent with the National Incident Management System (NIMS), the CSOP requires the designation of a primary lead. Larger jurisdictions may identify multiple leadership positions, but the Access Program Manager is the primary coordinator for the program.

An Emergency Access Program is "activated" in order to be utilized by all stakeholders. This action is carried out by the legal authority authorized for [jurisdiction]. This "activation" is the formal direction that the program will be utilized for a specific time frame (EVENT) or for a specified duration (year, month, etc.)

In order to activate the Access Program according to this CERRA Standard Operating Procedure, there may need be a formal declaration of a state of emergency either by the local/statewide Emergency Manager or by a local/statewide elected official. (Note: The pre-requisites of "Activation" should be determined with the local authority and documented in this CSOP. The required process varies according to state and local law.) An emergency declaration will result in a communication by various parties including Access Program representatives notifying all stakeholders that a form of Access (reentry, commercial event, etc.) will be initiated.

3.0 Establishment of Governance Board Process

An Access Program is a cross-jurisdictional, cross-sector, cross-government effort. Successful implementation requires the active and engaged participation of stakeholders within [jurisdiction]. A Governance Board is the coordination of these stakeholders. It is designed to provide mechanisms to ensure the Access Program is best serving the needs of [jurisdiction] and its communities.

Governance Board processes will vary in size and make-up based on the local jurisdiction, the structure of the government, and the critical infrastructure sectors that form the backbone of the local communities. The governance board can be comprised of a formal collection of representatives from [jurisdiction] or an added responsibility for previously established groups (e.g. Local Emergency Planning Committee).

The Governance Board responsibilities are:

(4) To establish a collaborative environment to develop, review, and approve the initial CERRA SOP for program implementation,
(5) Maintain on-going review, coordination, and cooperation via regular meetings.
(6) To establish a forum for which stakeholders can raise issues and new requirements that may need incorporation into the SOP for best implementation of the program.

Governance Boards should include sufficient membership to ensure representation of all key government entities, including state or regional authorities (if implementation of the program requires their support and/or coordination), but limited to be an effective body. The Access Program Manager, designated under the Authority section, will define a small group representing the key Emergency Management, Law Enforcement, and Critical Infrastructure representation to lead the Governance Board.

The primary goal of the Governance Board is the definition and maintenance of [jurisdiction] SOP. Development of organization specific instructions and/or general orders should remain the responsibility of the various organizations.

For [Jurisdiction], the program Governance Board will consist of:
[List by roles/positions & names]

4.0 Roles and Responsibilities

In support of implementation of an Access Program, the following section will assist in defining the roles and responsibilities of the various coordinating parties within [jurisdiction]. The Governance Board can also publish specific direction on these roles and responsibilities in order to further define any specific areas.

The CERRA approach defines a set of 'roles' to best coordinate the Access Program support components:

- Definition and Coordination of Access
- Access Control
- Implementation (Activation) of Access

In this Standard Operating Procedure, these roles will be defined in the following context:

- Access Program Manager (Definition/Coordination of Access)
- Law Enforcement (Access Control)
- Response and Recovery Organizations (Implementation of Access)

A more detailed outline of the roles and responsibilities for these elements is provided below:

4.1 Access Program Manager

The Access Program Manager for the [Jurisdiction] Access Program is: [Insert Name]

The Access Program Manager's role is to manage and coordinate the response and recovery elements required for emergency events within the jurisdiction. Within this Access Program this role includes the preparation steps of defining access levels, approving organizations for entry, and pre-staging EVENT templates for activation as needed. It is the responsibility of the Access Program Manager to ensure that this information is communicated to all parties. This ensures that the Access Program Manager is able to manage and coordinate the access state for emergency events, including the level of access and response required during each phase of response and recovery effort.

4.2 Access Control (Law Enforcement Officers)

The Access Control role for this jurisdiction will be fulfilled by the following agencies:
[Insert Agency Name(s)]

The Access Control role within an Access Program is to manage the points of access (i.e. Checkpoints, Spot Checks) and to facilitate the assets and personnel entering or exiting a secure/restricted area. The Access Control responsibility includes responsibility for training and coordination for any personnel controlling access to the restricted zone, including review and

evaluation of access placards. The Access Control role works in coordination with the Access Program Manager to maintain cognizance of the access levels, defined restricted zones (geographies), and to ensure communication/coordination with all checkpoint personnel.

Within the CERRA approach, the Access Control Leads and Access Program Manager communicate and coordinate throughout the process via established procedures and the Emergency Operations Center (EOC). The CERRA Clearing House provides mobile applications that allows real-time coordinate across these vital roles. These applications are offered to jurisdictions to support seamless coordination and communication during activation.

The Access Control role in this Standard Operating Procedure is designated as the local law enforcement entity, with augmented support by requested state law enforcement (Department of Public Safety) resources.

4.3 Response and Recovery Organizations

Response and Recovery Organizations are the entities that may require access to an emergency zone to support the economic recovery of the affected region. These organizations include both stakeholders within [jurisdiction], out of jurisdiction supporting entities, and all applicable Critical Infrastructure (CI) and Business sectors. Through coordination with the Access Program, these organizations are responsible to ensure that the individuals requiring access have met appropriate identification, membership/affiliation, role, and qualifications requirements defined by the local access rules. These requirements are set based off of the event and response/recovery needs at a specific time.

All organizations in the below categories are approved by the Access Program Manager for access into [jurisdiction]. These organizations can be identified at a checkpoint or access entry location by a preapproved CERRA access credential or, in certain situations, vehicle markings/predefined identification issued by the local jurisdiction.

Response and Recovery Organizations fall into four (4) categories:

(5) Local Organizations – These organization are based within, or near to, the jurisdiction, and have local facilities, personnel, and/or assets. Local organizations will be known to the local Access Program Manager and participation, through the local enrollment process to ensure the timely access of personnel back into the area. Organizations in this category are required to register for CERRA access credentials with the Access Program.

(6) Regional/National Organizations – These organizations may have local facilities, personnel, and assets, but operationally provide support to response and recovery efforts through personnel based outside of the jurisdiction (e.g. Chevron, Walmart). Organizations in this category will comprise various sectors but traditionally be private and responding in order to recover and restart their facility operations. These organizations are known to the Access Program Manager, but the individuals requesting access will be identified and dispatched, often in real-time throughout the event.

Organizations in this category are required to register for CERRA access credentials with the Access Program and eligible for nationwide CERRA interoperable access credentials.

(7) Response Organizations – These organizations represent emergency services (and emergency support) organizations dispatched to the affected area (usually with agreement of the local authority) to provide augmentation support to the impacted emergency services. Organizations falling under this designation may be both public and private but generally respond in a life-saving or essential services capacity. Organizations in this category may register for CERRA access credentials into the Access Program or be identified by marked vehicles and/or previous local instruction.

(8) Response and Recovery Support Organizations – These organizations do not have local facilities, personnel, or assets, but operationally provide support to communities through pre-existing, or just-in-time, contractual relationships. These organizations may be known to the Access Program Manager and are approved for entry when a valid reason for support is demonstrated. These include private organizations both contracted by a local jurisdiction and those that are supporting other resources. Organizations in this category are required to register for CERRA access credentials with the Access Program and eligible for nationwide CERRA interoperable access credentials.

The overall objective of the CERRA coordinated approach is to enable all organizations to receive expedited access into emergency zones as necessary. Organizations that register for CERRA access credentials are utilizing the CERRA Clearing House and a local CERRA provider to ensure expedited access into the local jurisdiction. These organizations may also request access to other jurisdictions throughout the nation, and those access decisions have no effect on the access decision made by the local jurisdiction or Access Program Manager.

Organizations will utilize the local CERRA provider in coordination with the CERRA Clearing House to manage individuals and coordinate access with any participating jurisdiction. The CERRA Clearing House exchanges information with the local CERRA provider to determine access approval and generate and distribute access credentials as requested.

4.4 Use Cases/Access Requirements

The objective of an Access Program is to facilitate the expedited access of critical response and recovery assets to enable safer, more secure, and more effective return to normalcy for the community. This is both a security priority and an economic imperative. The below section includes template Use Cases as well as unique Access Requirements for this jurisdiction.

Use Cases

This Standard Operating Procedure includes two predefined Use Cases, or access templates, and will be utilize for potential events. This Use Cases are intended to be generic for their broad application to multiple potential events under the same event category. All information not outlined in the below Use Cases, is considered to operate the same as Standard Operating

Procedure or is defined within the CERRA Online Application in conjunction with the CERRA Clearing House and a local CERRA provider.

Use Case Access Template

EVENT Designation:
Activation Requirement:
Geographic Activation Area:
Access Program Manager:
Access Control: Local Jurisdiction Law Enforcement
Predefined Access Control Points (Checkpoints):

- [Text]

Initial Access Level:
Activation Communications Resources:
Access Credentials (One is Required): CERRA Access Credential, Marked Utility Vehicle/ID, Marked Emergency Response Vehicle/ID

Access Requirements

This Standard Operating Procedure includes Access Requirements that are used to define specific rules required for receiving access into this jurisdiction. Any rules not covered below, fall under the Standard Operating Procedure included in other sections.

Access Credential Requirements

In terms of Access Credentials, personnel requesting access into a secure area are separated into two groups: Emergency Responders, Response and Recovery Organization.

Emergency Responders are personnel who represent local law enforcement, local fire departments, the local/regional [Utility Company Designation], local emergency response designated government employees, and all other organizations that fall under the Emergency Services Sector. These organizations are able to identify themselves at an Access Point (Checkpoint) by using **one** the following means:

- Marked Vehicles
  - Local/Regional Emergency Responders must have their agency's name clearly marked on their vehicle with additional identification available if requested.
  - The Local/Regional [Utility Company Designation] falls into this category, any vendor/contractors must either come in a [Utility Company Designation] marked vehicle or register for a CERRA Access Credential.
- Emergency Responder ID
  - Local government employees designated as "Emergency Responders" on their jurisdiction issued ID badge, may present this badge at checkpoints for access into a secure area.

- CERRA Access Credential
  - All above organizations can register for an Access Level 1 CERRA Access Credential to be preapproved to receive access into a secure area within [jurisdiction]
  - The CERRA Access Credential is provided by the local CERRA provider. Please refer to [Local CERRA Provider Website/Contact] for more information.

Note: All organizations in the above category fall under Access Level 1.

Response and Recovery Organizations are personnel who represent Critical Infrastructure, local businesses, regional/national organizations, and all other applicable commercial and/or public sectors. These organizations identify themselves at a checkpoint through the following means:

- CERRA Access Credential
  - All above organizations can register for an Access Level 1, 2, 3, or 4 CERRA Access Credential to be preapproved to receive access into a secure area within [jurisdiction]
  - Personnel receiving a CERRA Access Credential are required to carry one form of Government Identification with them to receive access
  - The CERRA Access Credential is provided by local CERRA provider(s). Please refer to [Local CERRA Provider Website(s)/Contact] for more information.

Note: The Access Control role (Law Enforcement) maintains the access decision at the checkpoint and can request additional documentation or additional identification as necessary.

Additional access requirements may be added to specific events within the jurisdiction at a later date. These access requirements may require additional training (ex. HAZMAT Certified) or a restriction on access to certain areas (ex. Military Base).

4.5 Access Program Management Role

An Access Program is operated under the Definition of Authority. An organization (or individual) is designated as the Access Program Manager.

The Access Program Manager is responsible for the implementation and operations of the program. The Access Program Manager operates the program in accordance with the SOP defined and approved by the Governance Board.

The Governance Board provides oversight and coordination support for the Access Program.

4.6 Access Program Training, Coordination, Implementation

Access Program Training, Coordination and Implementation is the responsibility of each of the stakeholder organizations. The CERRA National Governance Board and CERRA Clearing House provide support, tools, and technology to organize, implement, and operate the local Access

Program(s). Participation by Response and Recovery organizations is coordinated by the local CERRA provider selected by [jurisdiction]. The CERRA Clearing House works in conjunction with the local enrollment provider, requiring their compliance with the CERRA technical interfaces necessary to support implementation of the jurisdictional defined EVENTS, Access Levels, and CERRA Access Credentials.

4.7 Access Program Activation

The Access Program is 'activated' for usage by processes defined within the CERRA SOP instruction and the Definition of Authority. The Access Program Manager, upon activation, enables coordinated response and recovery with all registered stakeholders.

5.0 Access Levels

The Access Program utilizes a Phased Entry approach, which allows for the definition of groupings, known as Access Levels, that are designed to generally correspond to the conditions within the restricted zone. During a crisis, or emergency, these might align with the level of stability and security expected within the zone in the periods following the event. When in use for crowd size events (sporting match, festival, protest, etc.) they might align with the level of security access the designated authority wants to maintain within the zone. In either scenario, the Phased Entry approach provides a mechanism for the Access Program to establish requirements which personnel and resources must meet to gain approval for access and a straightforward process to implement these restrictions. Within the Phased Entry approach, the Access Program defines specific rules to enable Access Authorization.

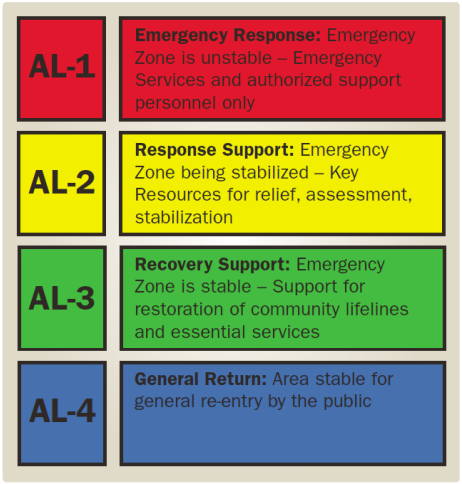


Figure 5.0.1-1 © Pegasus Research Foundation 2018

The CERRA Phased Entry access levels (used for crisis/emergency events) are provided in Figure 5.0.1-1.

The Phased Entry approach is utilized to provide a flexible toolset for Access Program Managers to define access restrictions in terms of the conditions within the restricted zone, while enabling Organizations to map response and recovery resources to these conditions ensuring the right personnel can gain access at the appropriate time period.

Q; Based on your scenarios, are their adjustments to the mapping of Access Levels (AL) to the specific capabilities needed for response & recovery? Document these to implement in your configuration.

5.1 Access Level Rule Elements

Access Levels are defined to enable jurisdictions to make better access decisions. The approach defines a set of required identity attributes that, when validated, verified, or vouched, enable the automated satisfaction of the rules defined within the program and the immediate approval of access and access tokens.

This Standard Operating Procedure leverages the CERRA approach and existing CERRA Access Programs to define standardized Access Level rules.

Access Level	Attribute Element	Description/Requirement	(M) / (O)
AL-1	Identification	Valid Government-issued Photo-ID Valid Access Level 1 CERRA Access Credential Valid Organization Issued Badge Marked Emergency Response Vehicle Marked [Utility Company Designation] Vehicle Local Government Emergency Responder Badge	M M O O O O
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-1 Response/Recovery personnel	M
AL-2	Identification	Valid Government-issued Photo-ID Valid Access Level 2 CERRA Access Credential Valid Organization Issued Badge	M M O
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-2 Response/Recovery personnel	M
AL-3	Identification	Valid Government-issued Photo-ID Valid Access Level 3 CERRA Access Credential Valid Organization Issued Badge	M M O
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-3 Response/Recovery personnel	M
AL-4	Identification	Valid Government-issued Photo-ID Valid Access Level 4 CERRA Access Credential	M M
	Membership	Vouched membership in Approved Organization	M
	Role/Capability	Approved AL-4 Response/Recovery personnel	M

Mandatory (M)/ Optional (O)

5.1.1 Identification

Organizations and personnel responding during an event must present the mandatory identifications required at a checkpoint into a secure area. The mandatory identifications listed above are those that the Access Control role (Law Enforcement) are trained to identify a checkpoint. These credentials may be verified by either visual inspection, a mobile/desktop application, or a direct support line.

The Access Control role may request both mandatory and optional credentials at a checkpoint, and the standing recommendation will be to bring all possible forms of identification within a desired Access Level when responding to an event.

Please refer to Access Requirements in Section 4.4 for further information on required formats or additional access requirements.

5.1.2 Membership/Affiliation

All personnel that request access within the Access Program will be required to be a member of or have an affiliation with a responding organization. The organization must vouch for all personnel that are designated for response purposes, and those personnel must bring their approved access identification to demonstrate their membership/affiliation.

The CERRA Approach, in conjunction with the CERRA Clearing House and a local CERRA provider, gives organizations the ability to vouch for personnel and allow their personnel to create CERRA Access Credentials to demonstrate a membership/affiliation. Organizations must register and vouch for their personnel through CERRA, unless they meet one of the other listed Access Requirements in Section 4.4.

5.1.3 Roles/Capabilities

Organizations will assign specific roles and capabilities to their personnel when responding to an event. These roles/capabilities are designed to inform both the Access Program Manager and Access Control of their purpose for responding to the local jurisdiction.

The Access Program Manager will be given all assigned roles/capabilities of personnel within [jurisdiction] to assist in informing access decisions. The CERRA application will be used by the Access Program Manager to utilize a [jurisdiction] specific dashboard in order to manage these roles/capabilities in an expedited manner.

5.1.4 Permission

Permission is the approval of the Organization for a specific employee (or contractor) to respond to an EVENT. Many personnel **may** meet the Access Level requirements established by [jurisdiction] for an EVENT, but the Organization will only designate (approve) those individual for necessary to affect the required response and/or recovery mission. The concept of permission ensures that (a) only those individuals required by the Organization respond limiting the risk to its employees and business and (b) that the Organization respects the direction of [jurisdiction] by only having required resources active during the EVENT.

5.1.5 Access Level Definition

The Access Level's for this Standard Operating Procedure are defined in the below table. These definitions outline the organizations expected to respond during an event, and the Access Level

that they will be designated. These Access Level definitions are subject to change based on the event, and organizations may have personnel in their organizations who receive different Access Level approvals based off of their designated role/capabilities.

The Phased Access process for this Standard Operating Procedure follows the standard CERRA guidelines. Please refer to Figure 5.0.1-1 for general access level references.

Access Level	Description/Requirement
Access Level 1 – Emergency Response (RED)	Emergency Responders • Fire Departments • EMS • Local, State, Federal Law Enforcement • Search & Rescue • Local Jurisdiction Designated Emergency Response Personnel Military (Including National Guard and Coast Guard) [Utility Company Designation] Essential Medical Personnel (ESF-8) Critical Infrastructure/Key Resource Essential Response Teams Critical Infrastructure Lifeline Sector Essential Response Teams Other personnel at the approval of the jurisdiction
AL-2 – Response Support (YELLOW)	Critical Infrastructure/Key Resource Response Support Personnel • Vendor/Contractor Organizations of Response Support Personnel • Damage Assessment Teams Critical Infrastructure Lifeline Sector Response Support Personnel • Damage Assessment Teams Security Organizations Official Damage Assessment Teams (FEMA, State, Local) Private/Public Sector Organizations Response and Damage Assessment Teams Voluntary Organizations Active in Disaster (VOAD) Response Teams Insurance Provider Damage Assessment Teams Other personnel at the approval of the jurisdiction
=AL-3 – Recovery Support (GREEN)	Critical Infrastructure/Key Resource Recovery Personnel • Vendor/Contractor Organizations Critical Infrastructure Lifeline Sector Recovery Personnel Private/Public Sector Organizations Recovery Personnel Voluntary Organizations Active in Disaster (VOAD) Recovery Teams Other personnel at the approval of the jurisdiction
AL-4 – General Return (BLUE)	General population return Other personnel at the approval of the jurisdiction

5.2 Access Approval

Access Approval and preapproval into [jurisdiction] will be decided by the Access Program Manager. All Access Approval request must be decided by the jurisdiction prior to an organization or their personnel receiving entry into a secure area. These approvals will allow the organization to produce CERRA Access Credentials or receive access via the other established access requirements.

The Access Program Manager can utilize the CERRA Application as well as predefined access best practices to expedite the jurisdiction access approval decisions.

Access Control personnel (Law Enforcement) will retain the final decision for access at checkpoints into a secure area. These personnel can use their discretion to accept or reject pre-approved access decisions if necessary.

6.0 Preparation - Coordination

In response to a potential event there is pre-incident coordination required between the local jurisdiction, Access Control personnel, Access Program Manager, and response/recovery organizations. This process is defined below to ensure a smooth transition from pre-incident to activation.

6.1. Access Registration/Maintenance

- Personnel requiring access and not meeting any predefined Access Requirements must pre-register for CERRA Access Credentials to ensure they can receive access during an event or post event.
    - The CERRA Access Credential registration is made available through a local CERRA provider working in conjunction with the CERRA Clearing House. Please visit (https://cerraaccess.org) for more information.
- Organizations must update and perform routine maintenance on their preregistered personnel roster to ensure that all appropriate personnel are registered, affiliations/memberships are identified, and roles/capabilities are assigned.
    - **Affiliation/Membership Example:** Employee/Employer registers and vouches for their response teams to receive CERRA Access Credentials.
    - **Role/Capability Example:** An Organization identifies their personnel as a "Damage Assessment Team" and assigns that role on their CERRA Access Credential.
- Pre-Identifying essential personnel and their Access Levels.
    - Organizations must be notified of their requirement to register for CERRA Access Credentials or their ability to meet other predefined Access Requirements within the local jurisdiction.
- Preparing Vehicle Placards, Letters of Access (LOA), or Mobile Placards for essential personnel
    - [Jurisdiction] is required to prepare, maintain, and distribute Placards that meet the criteria defined by the CERRA Clearing House. In order for these Placards to be CERRA compliant they must integrate with the CERRA Clearing House (https://cerraaccess.org)
    - A local CERRA provider will be designated to provide these Placards, distribute them, and maintain them on a yearly basis at no-cost to the jurisdiction.

6.2 Access Control (Law Enforcement) Preparation

Access Control personnel (Law Enforcement) will also require coordinated pre-incident preparation to ensure they are able to establish the appropriate checkpoints and identify organizations approved for access into [jurisdiction].

The pre-incident coordination for Law Enforcement will predominantly focus on communicating predefined checkpoint locations (see: Section 3.4) and distributing training materials to ensure that the Access Requirements and Identifications are understood and able to be executed on during an event.

It is the responsibility of the local jurisdiction and Access Program Manager to assist in law enforcement training coordination for their jurisdiction. The materials for this training can be created and distributed by a local CERRA provider in conjunction with the CERRA Clearing House.

Q; Do you want to identify or cite any specific procedures for post-evacuation access or event access in this section? (i.e. Muster points, or specific procedure that would be relevant to access control preparation).

6.3 Registration of Interest (ROI)

Organizations are required to register interest into jurisdictions they wish to receive access to. These organizations must some their Registration of Interest to the Access Program Manager so that they can receive an access decision. Organizations can submit this registration of interest before, during, or post event and the Access Program Manager can approve or disapprove the organization based on the information provided.

The Access Program Manager can choose to utilize the CERRA Application dashboard and a local CERRA provider to receive, organization, and coordinate these registrations of interest and access decisions.

7.0. Organization Registration – Enrollment Provider(s)

This Standard Operating Procedure designates a CERRA Enrollment Provider(s) that can assist in the coordination of the program, registration of organizations, and outreach/training for [jurisdiction]. The Enrollment Provider's responsibility is to work in conjunction with the CERRA Clearing House to ensure that the jurisdiction is provided all the necessary resources for an Access Program at no-cost, while also ensuring the jurisdiction is able to integrate nationally with the CERRA Clearing House.

The designated CERRA Enrollment Provider(s) for this jurisdiction is: [Insert Provider Name Here]

CERRA Enrollment Provider(s) for the jurisdiction will handle or assist with the following responsibilities:

- Organization Registration
  - The designated CERRA Enrollment Provider(s) will provide a platform to register organizations for access decision approvals and CERRA Access Credentials.
- CERRA Access Credential Creation/Distribution
  - The designated CERRA Enrollment Provider(s) will organize, create, and offer a method of distribution for CERRA Access Credentials.
- Private/Public Sector Outreach
  - The designated CERRA Enrollment Provider(s) will assist in public and private outreach campaigns, events, and other meetings to ensure the jurisdiction understands the required procedure for the Access Program.
- Law Enforcement Training
  - The designated CERRA Enrollment Provider(s) will assist in distributing the materials for law enforcement training as well as offering individual sessions to assist in training throughout the year.

8.0 Checkpoint Operations

Checkpoints are defined as access points utilized by law enforcement or Access Control personnel designed to control access into a secure or restricted area. In the CERRA Standard Operating Procedure, Checkpoints are operated by Access Control personnel (Law Enforcement). There are three types of operational checkpoints that may be used in order to control access into an area.

- Outer Checkpoints
  - Outer Checkpoints are access points established at the furthest point outside of a restricted or secure area to facilitate the controlled access of personnel and vehicles. These checkpoints are designed to be used for expedited access into a secure area by quick identification of CERRA Access Credentials or other associated access points.
  - Outer Checkpoints are set with the lowest required Access Level into [jurisdiction]. This is to ensure that no other Inner Checkpoints conflict with the Outer Checkpoint access level, and to allow a seamless transition between Access Level's for responding organizations.
- Inner Checkpoints
  - Inner Checkpoints are access points established within a restricted or secure area in order to further control access to the least stable areas within [jurisdiction]. These checkpoints are staged in areas that require more restrictive access (higher access level) and/or are unsafe for general response personnel to enter.
  - Inner Checkpoints will always be designated at least one access level higher than the established Outer Checkpoints. These checkpoints may require a more

detailed or scrutinized review of an individual's CERRA Access Credential or other Access Requirements due to the unsafe nature of the restricted area.

- Spot Checks
  - Spot Checks are access points that are implemented in a roaming capacity to ensure individuals who are within a restricted area meet the appropriate access requirements or have a CERRA Access Credential. These are designed to ensure that no unauthorized personnel are accessing restricted areas during an event.
  - Spot Checks are used to verify that an individual had the appropriate access level to pass through an Outer or Inner Checkpoint and are implemented at law enforcement's discretion or by the request of the Access Program Manager.

9.0 Activation

Activation is the process of activating the Access Program in preparation for or response to an Event. The process for designation of a jurisdictional authority for activation is discussed in Section 2.0: Governance the process and steps for activating the program once authority has been given are outlined below:

Designating an event

- The Access Program Manager must designate the appropriate event for activation. An event can range from an emergency situation to any type of event within [jurisdiction] that would require restricted or controlled access. This event must be designated in a pre-approved format that is made visible on the CERRA Access Credentials. [Jurisdiction] may choose to use a CERRA compliant provider to designate the event status.

Approving access

- The Access Program Manager must preapprove access for organizations requesting entry into a secure/restricted area during an event. These access decisions must be communicated to the organization and made visible on the CERRA Access Credentials. Organizations that meet the other Access Requirements for Access Level 1 defined in Section 3.4 are eligible to receive automatic preapproval. [Jurisdiction] may choose to use a CERRA compliant provider to organize and approve access decisions.

Creating and distributing access credentials

- Access Credentials must be distributed to organizations requesting access into [jurisdiction]. These credentials must meet the format outlined by the CERRA Clearing House and must be distributed pre-event. [Jurisdiction] may choose to use a CERRA compliant provider to create and distribute these credentials.

Establishing checkpoints

- The Access Control personnel (Law Enforcement) are responsible for establishing checkpoints according to Section 8.0 and following any predefined Use cases outlined in Section 3.4. [Jurisdiction] may choose to use the CERRA Application Dashboard to denote the checkpoint locations.

9.1 Event Updates

The Access Program Manager is required to update the event status and communicate those updates to the Access Control personnel and response and recovery organizations. These updates include the following:

- Access Level Changes
- Checkpoint Location Changes
- Additional Event Restrictions (HAZMAT, etc.)
- Event Activation Status (Active, Inactive, etc.)
- Event Duration Status
- Curfew Status

All of these updates must be communicated to all applicable stakeholders within [jurisdiction] to ensure seamless coordination during the reentry process. [Jurisdiction] may use the CERRA Application and a local CERRA provider to coordinate all of these updates.

9.2 Updated Access Credentials

Access Credentials must be updated to match the Event Updates or other associated criteria. Please refer to section 9.1 to understand what areas of the access tokens must be updated when Event Updates occur within [jurisdiction].

9.3 Enable Just-in-Time Access

Access Credentials must be available for immediate distribution for organizations who require "Just-In-Time" access. These organizations are ones that respond immediately post-event, and do not have the ability to identify personnel or vehicles until they are dispatched for a response effort.

The Access Program Manager must either have an interface to distribute these Placards to establish defined muster points during activation where Access Credentials can be distributed to incoming personnel. [Jurisdiction] may utilize a CERRA enrollment provider to manage the Just-In-Time delivery of CERRA Access Credentials.

10.0 On-Going Operations and Refinement

This Standard Operating Procedure will go through a routine update and refinement process to ensure that any new requirements, use-cases, or other stakeholder inputs are included. These 'new' requirements may be requested from the CERRA National Governance Board to maintain interoperability or may be added to support local-only jurisdictional requirements that need to be accepted in order to refine operations of the Access Program.

The on-going operation and refinement process of this operating procedure will be handled collectively by the Access Program Manager and Governance Board defined in Sections 3.4.1 and 3.0.