SCTE | STANDARDS

Network Operations Subcommittee

SCTE STANDARD

SCTE 286 2023

Operational Practices for Gaining Access to Incident Areas

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interoperability, interchangeability, best practices, and the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at https://scte.org.

140 Philips Road
Exton, PA 19341

Document Types and Tags

☐ Specification	☐ Checklist	☒ Facility
☐ Test or Measurement	☐ Metric	☒ Access Network
☐ Architecture or Framework	☐ Cloud	☒ Customer Premises
☒ Procedure, Process or Method		

Document Release History

Release	Date
SCTE 286 2023	*10/10/2023*

Note: Standards that are released multiple times in the same year use: a, b, c, etc. to indicate normative balloted updates and/or r1, r2, r3, etc. to indicate editorial changes to a released document after the year.

Table of Contents

List of Figures

1. Introduction

1.1. Executive Summary

Natural and human-made hazards challenge even the most robust continuity plans. Safety, security, and communications are paramount to ensuring a timely restoration of critical infrastructure such as broadband networks and utility power. Coordination of personnel into and out of the impacted area is heavily dependent on a solid communications plan and an underlying infrastructure to support the plan. This operational practice outlines important techniques that can be leveraged to ensure safe passage into and out of the affected areas where technicians will transverse. The Communications sector is one of the seven FEMA designated community lifeline sectors for the United States.

1.2. Scope

This operational practice contains recommendations for working with local authorities such as police, departments of public works, National Guard and other governmental agencies to obtain safe and authorized passage into and out of disaster zones. Content includes the following items (in addition to supplemental material supporting this list):

1. Sample company letters
2. Purpose of company need to obtain access
3. Typical equipment needed in a disaster zone such as identification clothing

1.3. Benefits

During times of disruption, security is important and access across barriers are often in place to prevent injury or theft. Telecommunications are front and center during the process of restoration. Power, cable, police, fire, and local officials alike need to be able to communicate. Cable's services provide many of the backbone connections for frontline responders. This operational practice provides a foundation for obtaining proper access to response areas and reducing mean time to repair.

1.4. Intended Audience

Cable operators, outside plant/critical facility contractors, and equipment suppliers.

1.5. Areas for Further Investigation or to be Added in Future Versions

None at time of publication

2. Normative References

The following documents contain provisions which, through reference in this text, constitute provisions of this document. The editions indicated were valid at the time of subcommittee approval. All documents are subject to revision and, while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1. SCTE References

No normative references are applicable.

2.2. Standards from Other Organizations

None

2.3. Other Published Materials

No normative references are applicable.

3. Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

3.1. SCTE References

[SCTE 206] SCTE 206 2021, Cable Operator Business Continuity and Disaster Recovery Operational Practices

3.2. Standards from Other Organizations

No informative references are applicable.

3.3. Other Published Materials

CISA Access Coordination Request Letter
(https://www.cisa.gov/resources-tools/resources/cisa-access-coordination-request-letter)

FEMA National Response Framework
(https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response)

FEMA Emergency Management Tools for Practitioners
(https://www.fema.gov/emergency-managers/practitioners)

SCTE Emergency Management & Disaster Recovery Resources
(https://www.scte.org/information-page-index/scte-emergency-management-disaster-recovery-resources/)

4. Compliance Notation

shall	This word or the adjective "***required***" means that the item is an absolute requirement of this document.
shall not	This phrase means that the item is an absolute prohibition of this document.
forbidden	This word means the value specified ***shall*** never be used.
should	This word or the adjective "*recommended*" means that there *may* exist valid reasons in particular circumstances to ignore this item, but the full implications *should* be understood and the case carefully weighed before choosing a different course.
should not	This phrase means that there *may* exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications *should* be understood and the case carefully weighed before implementing any behavior described with this label.
may	This word or the adjective "*optional*" indicate a course of action permissible within the limits of the document.
deprecated	Use is permissible for legacy purposes only. Deprecated features *may* be removed from future versions of this document. Implementations *should* avoid use of deprecated features.

5. Abbreviations and Definitions

5.1. Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
EOC	Emergency Operations Center
ESF2	United States Emergency Support Function 2
FEMA	United States Federal Emergency Management Agency
FSA	forward staging areas
PPE	personal protection equipment
RRCC	FEMA Regional Response Coordination Center
SCTE	Society of Cable Telecommunications Engineers
SWEAT	sewage water electricity academics trash
US	United States

5.2. Definitions

Definitions of terms used in this document are provided in this section. Defined terms that have specific meanings are capitalized. When the capitalized term is used in this document, the term has the specific meaning as defined in this section.

Re-entry tier(s)	The use and evolution of a re-entry tier system for the gradual introduction of different resources into a post disaster zone has grown over the years but is by no means universal. In 2019, University of Texas researchers conducted a large-scale study in this area, determining that approximately 75% of participating jurisdictions incorporated a phased re-entry. In determining the suitability for personnel of any type to enter a disaster zone, "Render Safe" or similar type teams enter and assess the

	area, then make recommendations. How much "art vs science" is used in making these determinations varies greatly by organization. In multiple disaster scenarios in Louisiana, federal responders and state and local jurisdictions took advance of insights gathered from the "SWEAT" Tool, which stands for sewage, water, electricity, academics, and trash. The tool's ongoing development and future use has been strongly recommended in numerous studies and After-Action Reviews. Each of the five areas are assessed on a color code of black (indicating no capability or capacity), red (indicating very limited capability), amber (indicating functioning but not at full capacity), and green (indicating a function capability). This was developed by the armed forces for use in assessing community capabilities in Iraq and Afghanistan, it is now being modified for domestic purposes.
Render Safe Task Force	Many states and local jurisdictions have developed the standard that after a disaster, a Render Safe Task Force Team entry is phase 1, the initial phase of re-entry. In Georgia, for example, during this phase, teams from state and local response agencies, as well as private sector utility providers, gain access to impacted areas. The primary objective of operating personnel during phase 1 is to render the area safe for the first responders who will follow them to conduct life safety operations. Most likely, members of the Render Safe Task Forces are co-located immediately before re-entry operations begin in defined forward staging areas (FSAs). These teams are the first officials to enter restricted areas; therefore, re-entry permits will not be required (as the task forces will have embedded law enforcement officials). Nearly all personnel within this group man emergency response vehicles with obvious agency or company markings. Findings from the Render Safe Task Force inform the timing on the introduction of all following re-entry tiers. NOTE: Though many of the Render Safe Task Force descriptions follow very similar guidelines, "Render Safe" is not a universally agreed upon concept. The State of New Jersey, for example, specifies that Render Safe Task Forces apply to potential bombing and explosive responses.
first responder	The classification of resources as "First Responders" varies by location. Per US Code, the term "first responder" includes a firefighter, law enforcement officer, paramedic, emergency medical technician, or other individual (including an employee of a legally organized and recognized volunteer organization, whether compensated or not), who, in the course of his or her professional duties, responds to fire, medical, hazardous material, or other similar emergencies. NOTE: There are no specifics in US Code that specify first responders as being from the public or private sector.

6. Why Access Can Be Denied?

Local emergency management officials, often with support of local or state law enforcement or the National Guard, will regularly restrict access to disaster zones before any private sector resources are allowed access until safety criteria can be established. These efforts are often conducted by what is called the "*Render Safe Task Forces*."

This phase includes to:

1. Assess the current condition of flooding through the area and the nature of damage to infrastructure and structures.
2. Determine the nature of any gas leaks and spills and the condition of the power infrastructure.
3. Certify that roads and bridges are safe to navigate.
4. Determine if any hazardous materials are present in the area and what, if any personal protective equipment may be required.
5. Assess the needs of stranded populations and that life safety measures can be provided to them. Law enforcement control over these stranded populations is also a key consideration.
6. Assess the ability of law enforcement to assist the stranded populations and to support first responders into the affected areas.
7. Determine the potential for looting and other property loss risks based on damage to affected areas and nature of remaining populations to inform access restrictions.

Once the above criteria have been satisfied, officials may begin allowing access based on already established criteria. This may be throttled back slightly based on law enforcement and first responder ability to support any of the newly entering resources. As discussed in the next sections, these new entry crews need to provide a high level of self-sufficiency, so they are not a burden on law enforcement, first responders or on other community aid resources.

7. Emergency Management Framework

Responding to disasters and emergencies requires the cooperation of a variety of organizations; the larger or more complex the incident, the greater the number and variety of organizations that must respond. Think of a residential fire: Firefighters are leading the charge; public works may be on scene providing traffic control; police are providing security; emergency medical services personnel are triaging, transporting, and redistributing injured to local hospitals; and a local nonprofit or voluntary organization (e.g., American Red Cross and Salvation Army) may be on hand to assist displaced residents. For large disasters, such as major hurricanes or earthquakes, the incident complexity is increased as others—such as state, tribal, local, and federal government authorities—become involved. Businesses, voluntary organizations, and other elements of the private sector are also key stakeholders, providing the essential services that must be restored following an incident. The United States Federal Emergency Management Agency (FEMA) has published the National Response Framework that provides a foundation for how organizations coordinate, integrate, and unify their response.

Cable broadband providers play an integral role in supporting the response efforts by providing critical communication resources before, during and after incidents. This framework *should* be reviewed, and teams familiarized with the contents.

The responsibility for responding to natural and human-caused incidents that have recognizable geographic boundaries generally begins at the local level with individuals and public officials in the county, parish, city, or town affected by an incident. Cable broadband providers *should* develop clear lines of communication at the local level to help ensure timely access to information and resources needed to get proper access to impacted areas. Given the nature of our outside plant hybrid fiber coax infrastructure, the cable broadband industry can experience incidents at the local level on any given day. The industry is continuously developing and refining playbooks to be thoroughly ready for threats.

State governments supplement local efforts before, during, and after incidents by applying in-state resources first. When an incident expands or has the potential to expand beyond the capability of a local jurisdiction and responders cannot meet the needs with mutual aid and assistance resources, local officials contact the state. Cable broadband providers *should* also maintain relationships with state officials to

understand impacts of incidents and overcome obstacles that might be hampering access to offline cable broadband services.

Finally, the United States Federal Government becomes involved with a response when federal interests are involved; when local, state, tribal, territorial, or insular resources are insufficient and federal assistance is requested; or as authorized or required by statute, regulation, or policy. Accordingly, in some instances, the federal government may play a supporting role to local, state, tribal, territorial, or insular area authorities by providing federal assistance to the affected parties. Many cable broadband providers have teams responsible for maintaining necessary federal government relations. This relationship is vital to clearing barriers that may be imposed by federal jurisdiction during and after an incident.

Within the National Response Framework, the cable broadband industry is identified as part of Emergency Support Function 2 (ESF2) – Communications as well as one of the Community Lifeline units – Communications. Both dictate that the industry plays an integrated role to the other designees in these important response concepts. Community Lifeline units use a support decision-making framework (displayed in Figure 1) to help accelerate response and return to normalcy.

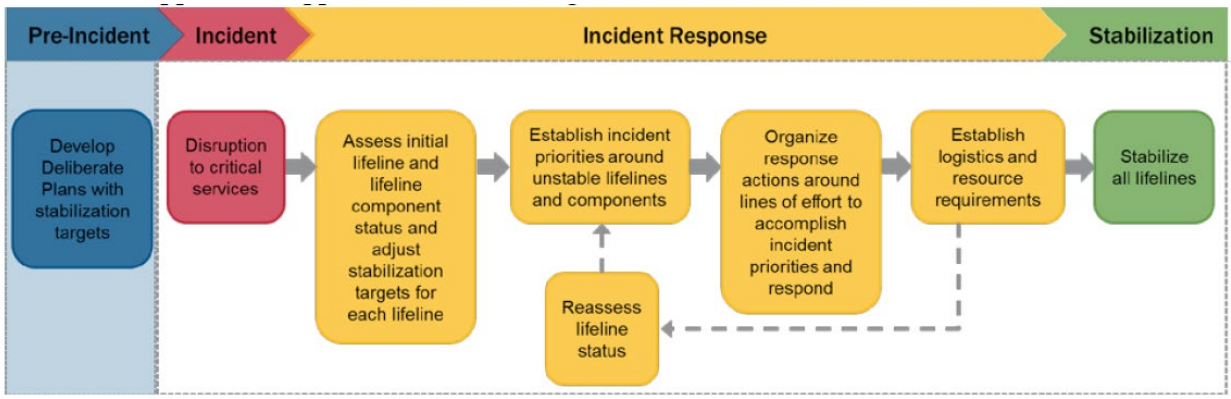

Figure 1 The Application of Community Lifelines to Support Emergency Management

Local, state, and federal dealings that are vital to consider as part of the response process include:

- whom providers deal with during events
- what are the local state and federal processes (common things)
- how things roll up from the ground zero incident zone, and
- when to even try to get beyond the control lines of area of impact.

Mitigation (blue sky planning) is vital to elevating readiness for response. The following list can enhance provider preparation:

- knowing who you need to speak with during events
- understanding the various states/differences where the problem occurs
- preparing the staging area for a predicted incident
- looking at event specific checklists
- drafting pre-season checklists for something like hurricane forecasted season
- response phase readiness while the incident is happening (what do we do while things are impacting the zone), and
- clearly defining how/when to mobilize response.

Finally, cable broadband providers have consistent needs during a response:

- fair and equal access to fuel,
- security of response teams, and
- proper access to impacted networks equipment needing restoration.

8. Requirements to Get Access

What do cable broadband providers need to have on hand to get clearance past the restricted zone? Lead responders have a primary role to keep citizens safe and society orderly during return to normal. Therefore, it is vital for providers or their approved response contractors to have one or more of the following devices that demonstrate a need to be crossing the safety line into impacted territory:

1. Company badge
2. Company access letter
3. Placards on trucks (including contractors)
4. Work order
5. Technology displaying access to the dispatch zone
6. Other governmental property pre-clearance (federal defense passes – military clearance pass)
7. Tribal land access requirements
8. DHS letter if issued

In short, technicians may encounter people whose role it is to limit access beyond a demarcation line and our intent with one or more of the eight items listed above is to safely and confidentially convince the individual(s) that the cable technician belongs in such a restricted zone.

9. Cable Operator Own Business Continuity in Response Areas

In section 9, it is asked, "How can providers be self-servicing/self-sustaining as a responding company and not a burden on the rest of response crews?" SCTE 206 [3.1], highlights general business continuity practices that *should* be reviewed and can provide a foundation for being ready for response. To demonstrate readiness for responding to disasters and getting past the caution tape, this list *should* be used as a basis of essential items:

1. Water
2. Food
3. Communications
4. Personnel and resource security
5. Transportation
6. Fuel
7. Roadside support of fleet
8. Chain of command
9. Medical support
    a. PPE
    b. Required inoculations
    c. First aid supplies
    d. Decontamination protocols
10. Tools and materials for scope of work related to response
    a. Foreign voltage detection tools
    b. Connectors
    c. Amplifiers
    d. Generators
    e. Nodes

f. Fiber
g. Coaxial cable
h. HFC power delivery hardware

11. Housing and personal relief facilities as needed for response individuals

Annex A. Sample Access Letter and CISA Access Letter

Note, the following is an example of language that your company could use to help achieve access into restricted restoration zones. Please customize as needed.

COMPANY LETTERHEAD

Company Name
Address Line 1
Address Line 2
City, State, Zip code
Main phone number

November 20, 2020

RE: Event name

Note 1: If CISA Access letter is published, use that exact name as event name.

Note 2: If only state level declarations are in place you might use…..

State of XXXXX Executive Order 17-235

State of XXX State of Emergency Declaration EM-3387

To Local, State, Federal Law Enforcement, Department of Highways and Transportation, and Emergency Management Agencies, Tribal Lands, National Guard

The bearer of this letter is an emergency responder or emergency team member carrying out communications enablement or communications restoration activities relating to critical infrastructure and vital resources or is a transportation carrier delivering essential equipment or supplies. Any **Company Name** employee, or contractor, presenting this letter is authorized access to assist in these network activities on our network, in our network facilities and/or our administrative buildings.

This employee, or contractor, is also required to present a personal photo I.D. and company identification.

Your cooperation is sincerely appreciated. If any further information or validation is required, please contact name 1, title and 24x7 phone number, name 2, title and 24x7 phone number, or name 3, job title and 24x7 phone number.

(NOTE: If a 24x7 Network Operations Center or other call center option is used, it is very important that anyone receiving an inquiry call is briefed on what to say and has the ability to verify identity).

Thank you,

Signature
Name of Senior Level Company officer/employee
Job title
Company name.
Office phone number

The Access Coordination Request letter (ACR letter) is provided to assist critical infrastructure owners and operators engage local officials in coordinating the access and support necessary to restore infrastructure services.

When warranted, CISA will post an ACR letter for and incident at this URL. If recovery activities continue beyond the effective dates, CISA will issue a new letter for that incident with new effective dates.

The following is an example of an access letter in support of a prior incident.

ACCESS COORDINATION REQUEST

California Atmospheric River Event

Effective 6 January 2023 – 31 January 2023

To: Federal, State, Local, Tribal, and Territorial Emergency Managers and Law Enforcement Officials

The Cybersecurity and Infrastructure Security Agency (CISA) requests your consideration in granting appropriate support to critical infrastructure sectors impacted by the **California Atmospheric River Event**. Previous response operations have shown critical infrastructure owners and operators routinely require area access, communication support, fuel priority, and may also require housing, and regulatory relief to assess damage, perform repairs, or implement mitigation measures necessary to restore services and functions essential for public health and safet**y.**

CISA requests extending this support to owners and operators of the following critical infrastructure sectors:

Chemical	Commercial Facilities	Communications*	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services	Energy*
Financial Services	Food and Agriculture	Government Facilities	Health Care and Public Health
Information Technology	Nuclear Reactors, Materials, and Waste	Transportation Systems	Water and Wastewater Systems

*Presidential Policy Directive/PPD-21 identifies communications and energy systems as "uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." In response to certain circumstances and incidents, these systems benefit from receiving priority and early support since they are foundational to the restoration of all other critical infrastructure.

This letter does not direct response operations, nor does it supersede the laws, regulations, guidance, priorities, access control measures, and actions established, by state, and local, tribal, and territorial emergency management and law enforcement officials or other proper authorities.

This letter is posted on www.CISA.gov and copies have been provided to the state Emergency Operations Center (EOC) and FEMA Regional Response Coordination Center (RRCC).

CISA can be reached 24-hours a day at 888-282-0870 or Central@cisa.dhs.gov.

ROBERT H DRUMM Digitally signed by ROBERT H DRUMM
Date: 2023.01.06 09:18:02 -05'00'

Robert H. Drumm Jr.
Associate Director for CISA Central, Integrated Operations Division
Cybersecurity and Infrastructure Security Agency

