Southern California Edison

All-Hazards Plan

Prepared by:
Business Resiliency
November 2022

Plan Technical Specialist:
BRDM

This Page is Intentionally Blank

Contents

Signed Concurrence

The *Southern California Edison All-Hazards Plan* approval signature page has been included to document changes and ensure version control.

The Director of the Business Resiliency Department authorizes all changes to the *Southern California Edison All-Hazards Plan*, agrees with the approach presented, and approves content. Change notifications will be sent to an authorized distribution list.

Agreed to and approved by:

______________________________ ______________________________

Donald Daigler, Director Business Resiliency
Southern California Edison

Date

Record of Changes

Date	Description	Completed By
12/21	Creation of All Hazards Plan, inclusion of GO 166 standards and criteria, SEMS, NIMS, and organizational response information	SCE Planning Team [redacted]
10/22	Added detail for Major Outage, Customer Restoration, FERC Standards of Conduct, Macro Messaging, Storm Detail	D Boston [redacted]

Record of Distribution

Date	Organizational Unit	Mode
12/21	All OUs through the Matrix	Electronic distributions, posting to internal portal
12/22 (anticipated)	All OUs through the Matrix	Electronic distributions, posting to internal portal

General Order 166 Standards Reference Table

GO 166 Standard	AHP Section
Standard 1	
Internal Coordination	Chapter 6
ISO Coordination	Chapter 6, Section 6.7
Media Coordination	Chapter 6, Section 6.13
Government and External Coordination	Chapter 6, Section 6.2, Section 6.7
Safety Considerations	Chapter 6, Section 6.2
Damage Assessment	Chapter 6, Section 6.15
Restoration Priority Guidelines	Chapter 6, Section 6.17
Mutual Assistance	Chapter 4, Section 4.4
Plan Update	Chapter 2, Section 2.8
Standard 2	
Mutual Assistance Agreements	Covered by SCE Mutual Assistance Agreements
Standard 3	
Emergency Training and Exercises	Chapter 5, Section 5.1
Standard 4	
Customer Communications	Chapter 6, Section 6.13
External and Government Communications	Chapter 2, Section 2.8 Chapter 6, Section 6.2, Section 6.7
Independent System Operator/ Transmission Owner	Chapter 6, Section 6.7
Standard 5	
Activation Standard	Chapter 6, Section 6.3
Standard 6	
Initial Notification Standard	Chapter 6, Section 6.7.3
Standard 7	
Mutual Assistance Evaluation Standard	Chapter 2, Section 2.6 Chapter 4, Section 4.4 Chapter 6, Section 6.6
Standard 8	
Major Outage Communication	Chapter 6, Section 6.13.10,
Standard 9	
Personnel Redeployment Planning Standard	Chapter 4, Section 4.5
Standard 10 **Annual Pre-Event Coordination Standard**	Chapter 2, Section 2.8 Chapter 5, Section 5.2.1 Chapter 6, Section 6.7.2, Section 6.13.9
Standard 11	
Annual Report	Annual Filing
Standard 12	
Restoration Performance Benchmark for a Measured Event	Chapter 6 Section 6.13.10

GO 166 Standard	AHP Section
Standard 13	
Call Center Benchmark for a Measured Event	Chapter 6 Section 6.13.10
Standard 14	
Plan Development, Coordination, Maintenance	Chapter 2, Section 2.8

1 Purpose and Scope

The Southern California Edison (SCE) All-Hazards Plan (AHP) outlines the company's approach to emergency management. The plan integrates the strategies set by the National Response Framework, mirroring the mission areas and the applicable core capabilities as defined by the Federal Emergency Management Agency (FEMA). It is in alignment with concepts identified in both the Standardized Emergency Management System (SEMS) and National Incident Management System (NIMS).

The AHP serves as the base document for strategic, operational, and tactical planning by building upon the capacities of the company and highlights the roles and responsibilities of each organizational unit (OU). It incorporates a hybrid of scenario, functional, and capability-based planning to identify courses of actions from a comprehensive risk analysis of the threats and all hazards within SCE's service territory. The AHP is a whole of company approach to continue operations and meet the diverse needs of the whole community in coordination and participation with our emergency response partners.

This plan outlines the roles and responsibilities for Incident Management Teams (IMT) during response operations. It is designed to help ensure safe and efficient restoration for any type of outage through consistent use of the Incident Command System, identification of applicable prioritization and restoration strategies, and the development of a common operating picture for communicating situational awareness to internal and external stakeholders. This plan does not supersede or replace existing procedures for safety, hazardous materials response, or other similar procedures adopted and in place, including and not limited to specific response plans prepared to address individual circumstances or to comply with regulatory requirements.

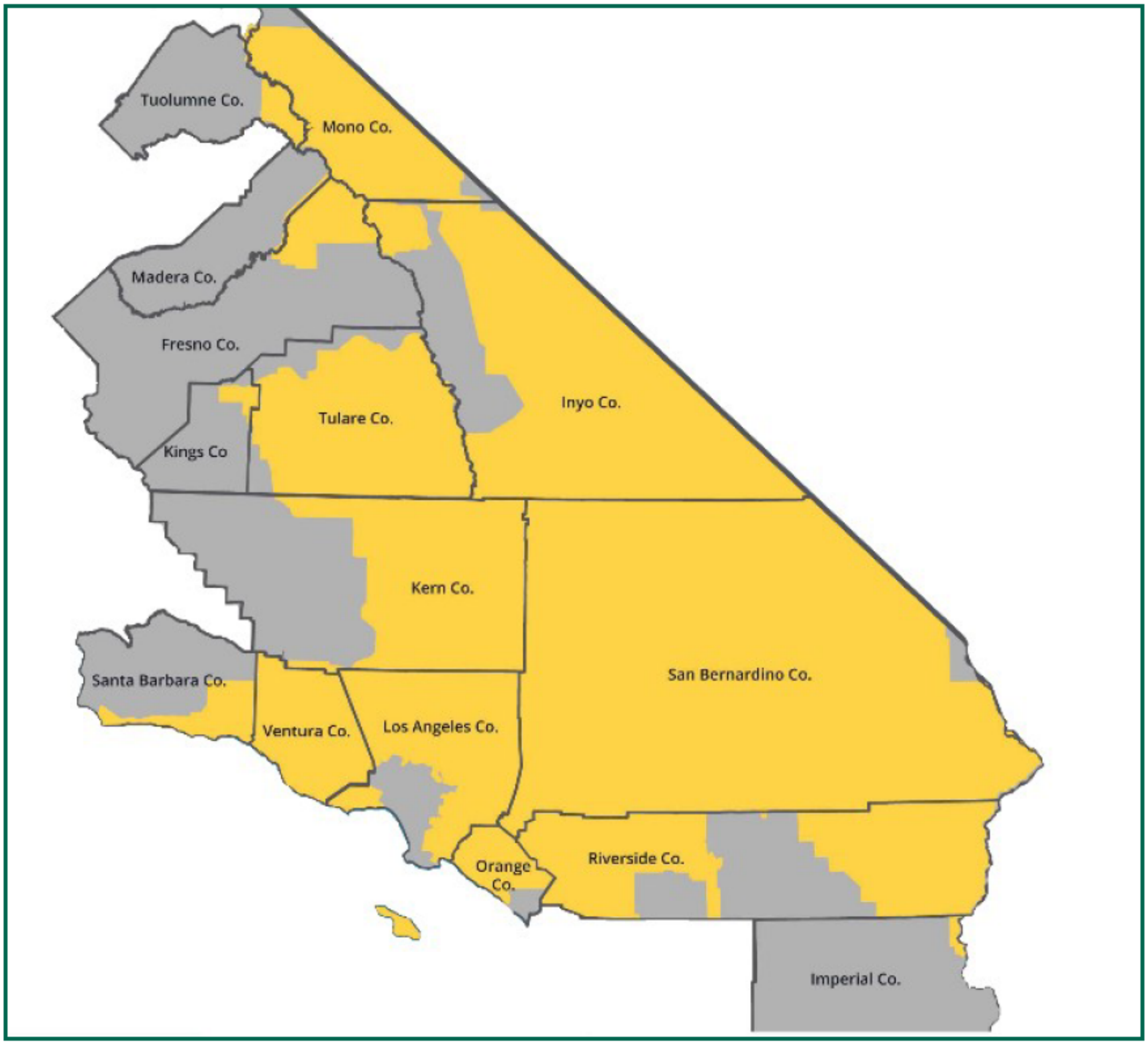
2 Situation Overview and Assumptions

2.1 Service Territory Profile

As one of the nation's largest investor-owned electric utilities, Southern California Edison delivers power to 15 million people in 50,000 square-miles across central, coastal and Southern California. SCE delivers more than 87 billion kWh of electricity and powers a total of 180 incorporated cities, 15 counties, 5,000 large businesses, and 280,000 small businesses. In addition to providing electricity to a large area in California, SCE also provides all utilities to Catalina Island including gas, electric and water. SCE's operations extend beyond this as well with Edison Carrier Solutions, which is a telecommunication operation that provides network capability to SCE and other commercial customers.

The SCE Service Territory is a dynamic and hazard rich environment. Within SCE's 50,000 square-mile footprint no community is immune from disaster; wildfires, floods, and earthquakes are common occurrences, and hold potential for large-scale impacts. While this area faces significant hazards, the SCE Service Territory is extremely diverse, and SCE strives to incorporate the Whole Community perspective in planning for these hazards. The Whole Community perspective ensures a shared understanding of the community needs before, during, and after an emergency, including populations with access and functional needs. Access and functional needs populations include, but are not limited to, individuals who have developmental or intellectual disabilities, physical disabilities, chronic conditions, injuries, limited or non-English speaking proficiency, older adults, children, or people living in institutionalized settings. Additionally, there may be individuals who are low income, homeless, or transportation disadvantaged who would be especially vulnerable to a power disruption.

Figure 1. SCE Service Territory Map



2.2 All-Hazards Approach

While incident types vary greatly, the potential effects of these incidents do not, and SCE addresses response planning through an all-hazards approach. SCE focuses on capabilities that are critical to address a full spectrum of disruptive events, including natural and/or human-caused emergencies.

SCE's All-Hazards Approach incorporates mitigation programs to reduce vulnerabilities to (disasters/emergencies/incidents), as well as the preparedness activities to ensure capabilities and resources are available for an effective response. SCE recognizes certain hazards require extensive attention and are further detailed in incident specific annexes to the AHP. SCE develops and maintains a portfolio of response plans.

2.3 Hazard Analysis Summary

SCE addresses a wide range of threats and hazards by developing an understanding of risks and identifying appropriate strategies to minimize vulnerability and impacts from known hazards. SCE's hazard analysis approach aligns with standard FEMA and California Office of Emergency Services (Cal OES) methodologies for hazard and risk assessment criteria to identify and profile hazards within the SCE Service Territory.

SCE's approach towards hazard analysis aligns with public sector hazard identification and risk assessments. Through this alignment, SCE can plan mitigations against known vulnerabilities and enhance community resilience throughout its Service Territory. In addition to SCE's planning efforts around natural and man-made threats and hazards, SCE also builds capabilities to address (business) industry-specific hazards.

Below are hazards for consideration based on the California State Hazard Mitigation Plan, and industry-specific threats unique to owners and operators of critical infrastructure.

Figure 2. Hazard Types

Natural	Business	Human-caused
– Drought – Earthquake – Infectious Disease – Heat Storm – Wildfire – Debris Flow – Landslide – Wind Storm – Flood – Tsunami – Winter Storm – Space Weather	– Dam Failure – Electrical System Failure – Utility caused fire – Utility caused injury or fatality – HAZMAT release – Vault explosion – IT Systems Interruptions – Communications Systems Failure – Business Continuity	– Active Shooter Incident – Physical Security incident – Civil Unrest – Biological attack – Chemical attack – Cyber-attack (data, infrastructure, DoS, Ransomware)

2.4 Storm Conditions, Major Outages, and Measured Events

The hazards listed above may create "Storm" conditions in the SCE service area. Storms are classified into four intensity levels: Mild, Moderate, Severe and Catastrophic. These intensity levels are established for SCE's entire service territory, as well as for individual districts. The overall incident intensity level is based on an aggregation of the district level information that has been augmented with consideration for widespread incidents such as transmission or substation interruptions.

SCE will base all prevention, mitigation, preparedness, response and recovery operations related to storm incidents on the following scenarios and potential impacts based on intensity:

Storm Classifications

Mild Storm

A mild incident is typically localized to districts within a single region and resources at the district or local level are sufficient to manage response and recovery activities. Mild incidents are frequent, occurring several times in one season. Such incidents can be characterized by average to slightly higher than average number of storm-related sustained incidents resulting in:

- Customer interruptions: Typically, less than 2.5% of total customers affected in a district or sector. Region or territory wide: the number of customers impacted is typically less than 1%.
- Restoration: Sufficient distribution, transmission, substation, and other design, construction, and maintenance resources can be deployed to provide assistance with extended shifts for personnel.
- Resources available within the locally impacted area or adjacent areas to respond (or equivalent area of responsibility for other departments).
- Majority of customers are typically expected to be restored in less than 24 hours.
- Resources required to repair damaged assets are typically readily available.
- Other significant events requiring an elevated response, as determined by management.

Moderate Storm

A moderate incident is typically spread over multiple districts or in a more intense isolated incident that requires additional resources to manage response and recovery activities. Moderate incidents are experienced only a few times in any one year. Such incidents can be characterized by a higher-than-normal number of storm-related sustained incidents resulting in:

- Customer interruptions: Typically, between 2.5-10% of total customers impacted in a district or sector. Region or territory wide: less than 2-3%.
- Restoration: Sufficient distribution, transmission, substation, and other design, construction, and maintenance resources from the surrounding Regions can be deployed / reallocated to provide assistance with extended shifts for personnel.
- Resources scheduled within the impacted areas or adjacent areas to respond (or equivalent area of responsibility for other departments).
- Majority of customers are typically expected to be restored in less than 48 hours.
- Resources required to repair damaged assets are typically available.
- Isolated damage to transmission or substation facilities within a local region.
- Other significant events requiring this elevation of response, as determined by management.

Storm Classifications

Severe Storm

A severe incident is typically either an incident with escalating impacts, affecting multiple regions or a severe intensity isolated incident. Such incidents are rarely experienced on a yearly basis, occurring on average once or twice every ten years and are characterized by an extremely high number of storm-related, sustained incidents resulting in:

- Customer interruptions: Typically, between 10-20% of total customers impacted in a district or sector. Region or territory wide: 5-10%.
- Restoration: Insufficient distribution, transmission, substation, and other design, construction, and maintenance resources. Assistance from non-adjacent areas may be required.
- Resource requirements (>100% of area resources) that affect multiple zones and require coordinated effort to manage response and recovery activities.
- Majority of customers are expected to be restored in less than 72 hours.
- Resources required to repair damaged assets may exceed those available.
- Extensive damage to transmission and/or distribution facilities.
- Other significant events requiring this elevation of response, as determined by management.

Catastrophic Storm

A catastrophic emergency or incident may require additional assistance if the resources required to respond exceed the available SCE resources and restoration may be prolonged beyond 72 hours. Such incidents are extremely rare and may cause such significant damage to the system resulting in:

- A company-wide need to focus on electrical restoration efforts.
- Customer interruptions: Greater than 20% of total customers affected in district or sector.
- Greater than 10% region or territory wide.
- Restoration: Insufficient distribution, transmission, substation, and other design, construction, and maintenance resources. Assistance from non-adjacent areas is required (>100% of SCE resources).
- Restoration may be prolonged beyond 72 hours and may require mutual assistance support.
- Resources required to repair damaged assets may exceed those available.
- Extensive damage to transmission and/or distribution facilities.
- Potential safety and/or health concerns.
- Other significant events requiring this elevation of response, as determined by management.

Potential Impacts
SCE facilities as a potential contributor to creating a hazardous condition
Service outages that may pose a life safety risk to critical care customers or essential services
Impacts to SCE facilities and employees
Limited access to damaged infrastructure, facilities and employees
Damage to critical dependencies such as gas, water, oil and telecommunications
Possible hazardous materials release

2.4.1 Major Outages and Measured Events

Both Severe Storms and Catastrophic Storms may meet the criteria for a Major Outage. Major Outages are defined in General Order 166, consistent with Public Utilities Code Section 364: a Major Outage occurs when 10% of the electric utility's serviceable customers experience a simultaneous, non-momentary interruption of service.

A Measured Event is a Major Outage resulting from non-earthquake, weather-related causes, affecting between 10% (simultaneous) and 40% (cumulative) of a utility's electric customer base. A Measured Event is deemed to begin at 12 a.m. on the day when more than one percent (simultaneous) of the utility's electric customers experience sustained interruptions. A Measured Event is deemed to end when fewer than one percent (simultaneous) of the utility's customers experience sustained interruptions in two consecutive 24-hour periods (12:00 a.m. to 11:59 p.m.); and the end of the Measured Event in 11:59 p.m. of that 48-hour period.

2.5 Mitigation Overview

SCE has long taken substantial steps to reduce the risk of threats and hazards and continues to proactively enhance operational practices and infrastructure through comprehensive mitigation programs. Many of the mitigation measures reduce long-term risk to SCE from hazards and their effects. SCE contributes towards Statewide hazard mitigation through collaboration with public safety agencies and infrastructure improvement initiatives.

- Lower hazard risks in local communities through infrastructure improvements, and enhanced training for emergency responders
- Integration with Cal OES through involvement with the California Utilities Emergency Association (CUEA)

SCE attempts to minimize losses and interruptions to service reliability through the development and implementation of customer and power system focused mitigation programs such as:

2.5.1 Demand Response

SCE offers a Demand Response (DR) program aimed to help customers save energy and money. DR programs provide incentives for reducing electricity use when demand for electricity is high. Customers can choose from a variety of DR programs through SCE and independent third parties who provide DR services.

2.5.2 Wildfire Risk Mitigation

SCE has a Wildfire Risk Mitigation approach, also known as PSPS Protocols which incorporate the below components:

Long-Standing Operational Practices

- Special procedures during Red Flag Warning

- Automated Recloser Blocking
- Restricted Work Practices
- Operation Santa Ana (joint patrol with fire agencies)

Investing in System Hardening of Electric Grid

- Fire-resistant Poles
- Covered Conductor
- Current Limiting Fuses
- Next-Gen Engineering Technology

Bolstering Situational Awareness Capabilities

- Fire and Severe Weather Monitoring
- Rapidly Advancing Analytics to Improve Weather Prediction

Enhancing Operational Practices

- Extra-Sensitive Relay Settings
- Public Safety Power Shutoff & Community Engagement
- Vegetation Management

Community Access and Functional Needs

- External Feedback and Consultation
- Customer Programs and Available Resources
- Customer Preparedness Outreach and Community Engagement
- In-Event PSPS Customer Communications

2.5.3 Seismic Resiliency Program

The SCE Seismic Resiliency Program executes assessment and mitigation projects to establish a corporate risk tolerance, with a goal of achieving seismic performance objectives according to accepted standards. SCE utilizes industry specific standards and best practices. As part of the assessment processes, the following criteria is met:

- Best available science and data[1]
- Vetted deterministic and probabilistic approaches[2]
- Tiered approach to assessments as follows:

[1] U.S. Geological Survey, Calif. Geological Survey, and their partners such as the Southern California Earthquake Center provide collaborative summary reports on an ongoing basis that form the basis for SCE's earthquake hazard and risk analyses that are used to prioritize mitigation projects.

[2] Examples of vetted deterministic approaches include use of the ShakeOut earthquake scenario, described here: ShakeOut Earthquake Scenario | U.S. Geological Survey (usgs.gov) and also the USGS BSSC set of earthquake scenario ground motions described here: BSSC2014 (Scenario Catalog) (usgs.gov). Please see references contained therein on the above web pages. The main example of a vetted probabilistic approach is the UCERF3-TD model, described here: https://pubs.usgs.gov/fs/2015/3009/pdf/fs2015-3009.pdf (USGS summary-level fact sheet) and here: Long-Term Time-Dependent Probabilities for UCERF3-TD (full text scientific article)

- Macro-level scoping assessment (FEMA P-154 and ASCE 41-17 tier 1)
- Deterministic site-specific assessments (ASCE 41-17 tier 2 & 3, FEMA P-58 & E-74)
- Probabilistic and System-Level Assessments (OpenSHA & fault-tree analysis)
- Geotechnical engineering and engineering geology reports as needed

SCE prioritizes work focused on life safety and service reliability through the standardized prioritization method. The focus areas include non-electric, electric, generation, and communications.

2.5.4 Climate Adaptation Approach

SCE prepares the organization for climate change and severe weather events by using a consistent companywide approach to assess and develop near-term, medium, and long-term mitigations for climate related vulnerabilities. SCE will:

- Utilize future climate projections and scenarios to supplement historical data that will inform business planning and operations
- Develop indicators and analyze trends to determine if future outlooks are coming to fruition and determine proper short- and long-term approaches. Integrate severe weather and climate change adaptation efforts into planning assumptions and recommendations
- Establish an internal strategy and external engagement plan that aligns with program and operational goals and addresses short, medium and/or long-term climate adaption impacts
- Ensure proper regulatory, & policy alignment, internally and externally, in relation to climate change adaption initiatives
- Actively participate in research aimed to inform implementation of climate adaptation analytics and mitigation strategies, focusing on supporting outcomes that are aligned with best practices for business operations
- Focus on impacts to customers, specifically those customers disproportionately impacted by the outcomes of climate change

2.6 Planning Assumptions

SCE is actively engaged in managing potential reliability and safety impacts from any hazard that may cause disruption to the electrical system by prioritizing damage assessment, restoring critical infrastructure and communicating with internal and external stakeholders to increase situational awareness.

Below are assumptions reflecting the situations to be considered to achieve effective emergency response:

- SCE will organize for and respond to a given incident following ICS, SEMS, and NIMS principles.

- All incidents are local, SCE must be able to initiate initial assessments, repairs, and response with little to no assistance.
- Incidents may occur at any time with little or no warning and may exceed SCE's capabilities. No-notice events may require immediate activation of an IMT to prioritize and manage response operations.
- Damage assessment operations will be performed when safe to do so.
- Restoration activities may need to be prioritized based on response operations.
- Emergencies may result in SCE employee casualties, fatalities, and displace employees from their homes.
- Individuals with access or functional needs may require resources or assistance from SCE.
- The greater the complexity, impact, and geographic scope of an emergency, the more coordination will be required.
- Mutual assistance and other forms of emergency assistance will be requested when SCE exhausts or anticipates exhausting its internal resources.
- SCE provides electricity, water, and gas services to Catalina Island. Incident response on Catalina Island is executed according to current plans, policies, and procedures.
- SCE Carrier Solutions is a fiber network privately owned and operated by SCE. SCE Carrier Solutions is subject to regulation under the Federal Communications Commission.
- Local jurisdiction EOCs may be activated to coordinate city, county and state government response to an SCE Storm incident.
- SCE personnel may be deployed to communicate and coordinate activities with city, county and state EOCs where necessary.

2.7 Regulatory Compliance, Standards and Authorities.

SCE abides by the regulations established by various regulatory agencies to ensure it provides affordable, safe, resilient, and reliable energy to its customers. At the enterprise level, SCE maintains a robust Ethics and Compliance organization responsible for governance and maintenance for all compliance requirements as imposed by applicable regulatory agencies. Additionally, Business Resiliency maintains a compliance and reporting organization responsible for governance and oversight specifically related to regulatory requirements of an emergency management nature.

Additionally, SCE identifies these applicable standards and authorities for the Incident Support Team (IST) and Incident Management Team (IMT) through the Incident Management Team Guidelines, and unique standards and authorities specific to incident types through the development of Incident/Hazard Specific Annexes to the All-Hazards Plan. In addition, the Crisis Management Council (CMC) or Officer-In-Charge may issue a delegation of authority to IST/IMT Incident Commanders to outline incident-specific authorities.

Multiple authorities guide the structure, development, and implementation of SCE's plans, policies, and procedures to ensure compliance adherence and proper documentation of processes and procedures to meet operational compliance as set forth by the regulatory agencies. SCE's compliance plans are in alignment with the requirements set by FERC, NERC, and the CPUC. The following requirements inform emergency plans and procedures:

- General Order Number 95 and General Order Number 128
- California Independent System Operator (ISO) Standards for Reliability and Safety during Emergencies and Disasters (December 1997)

[redacted]

- Federal Energy Regulatory Commission (FERC) – Under FERCs hydroelectric licensing, SCE is required to exercise the Hydro Emergency Action Plan (EAP) and Dam Safety Plan on an annual basis. FERC also has Standards of Conduct which SCE complies with. FERC Standards of Conduct are included in Appendix C and will be followed during all activations of the IMT/IST.
- California Public Utilities Commission (CPUC) – General Order 166. The CPUC established General Order-166 (GO-166) to ensure jurisdictional electric utilities are prepared for emergencies and disasters to minimize damage and inconvenience to the public which may occur as a result of electric system failures, Major Outages, or hazards posed by damage to electric distribution facilities. In alignment with GO-166 standards, SCE is committed to conducting annual emergency exercises and trainings that model the Emergency Response Plan.
- California Public Utilities Commission (CPUC) – Resolution ESRB-8 and Public Safety Power Shutoff (PSPS) guidelines. The CPUC established Resolution ESRB-8 and the requirements imposed under the Public Safety Power Shutoff (PSPS) Order Instituting Rulemaking (OIR) Phase 1 (Decision (D.) 19-05-042), Phase 2 (D.20-05-051), Phase 3 (D.21-06-034) and PSPS Order Instituting Investigation (OII) (D.21-06-014) to ensure that electrical utilities are specifically prepared to execute pro-active de-energization events that may be used by the utility to prevent wildfire ignition in designated High Fire Risk Areas (HFRA) and protect public safety.
- North American Electric Reliability Corporation (NERC) - NERC has been certified as the Electric Reliability Organization by FERC. NERC is the overall governing body who issues recommendations to the electric industry. NERC delegates authority to enforce reliability standards to eight regional Entities including Western Electricity Coordinating Council (WECC), SCE is within the WECC region.

2.8 Plan Development, Coordination and Maintenance

The AHP was developed as SCE's basic plan for all-hazards associated with an electric utility and with SCE's geographic service territory. The AHP discusses the overall approach to planning for, responding to, and recovering from all incident types. In addition to the basic plan, the AHP a includes functional annexes which identify specific information and direction for critical operational functions, and incident-specific annexes which address special planning needs generated by the subject threat/hazard/incident type.

Annually, SCE coordinates emergency preparations with state, county, and local agencies, as well as Essential Customers which is defined in General Order 166 as “Customers representing critical infrastructure and Public Safety Partners.” As part of this activity, SCE has a process for confirming and maintaining contacts and communication channels.

SCE’s plan development process includes considerations and lessons learned from recent incidents and events, coordination, and consultation with key internal and external stakeholders, and follows a regular annual update and maintenance cycle, in accordance with CPUC GO-166 standards. SCE will review its plan, following emergency activations to ensure activation and escalation standards are clear and appropriate. In addition, every two years, SCE will invite local government representatives to provide consultation as the plan is updated as well as the opportunity to comment on draft plans.

3 Organization

3.1 Business Resiliency Overview

These are the basic tenets of business resiliency that provide overall guidance, direction, oversight, and governance of SCE's most critical processes/systems to minimize impact from business disruptions.

3.1.1 Guiding Principles

- All Hazards Approach, with realistic and challenging scenarios
- Address Prevention, Protection, Response, Recovery & Mitigation
- Prioritize high risk concerns
- Adopt national standards
- Perform capability-based planning
- Resiliency initiatives directly tied to corporate goals
- Integrate external and internal stakeholders

3.1.2 General Responsibilities

- Develop and maintain an effective resiliency strategy
- Minimize the likelihood and impacts of a disruptive event
- Provide guidance and resources to respond and recover effectively and efficiently when an incident happens
- Provide coordination during all phases of an incident
- Determine next steps, and scale emergency response to organizational needs for any incident
- Implement a feedback loop that allows for lessons learned to inform improvements

Normal Operation

During normal operations SCE's Business Resiliency (BR) Organizational Unit leads the development of corporate level response plans and short-term recovery plans. BR also trains, equips, and exercise's the company's emergency response organization.

- Develop response and recovery plans
- Conduct training and exercise
- Escalate incidents whey they occur

Increased Likelihood

Once SCE is made aware there is an increased likelihood for an incident, BR through its number of internal capabilities such as, the Business Resiliency Duty Manager, Watch Office, and Situational Awareness Center is responsible for:

- Coordination of surveillance, detection, containment, and eradication activities

- Event escalation and/or de-escalation
- Identification and notification of key stakeholders
- Coordination of key stakeholders to ensure identification of adverse conditions

Credible Threat

Once an incident is deemed a credible threat, BR is responsible for the following:

- Coordination of pre-incident activities to include IST/IMT notification/communication, and enhanced situational awareness
- Assessment of incident complexity
- Organization of emergency response elements
- Escalation of incident
- Manage information sharing

Activation

Once a decision is made to activate for a response, BR is responsible for the following:

- Identification of appropriate emergency response organization (business continuity and/or disaster recovery teams, IST and/or IMT, CMC, Advance Planning Team)
- Coordinate notification, mobilization, and activation of emergency response organization
- Distribution of initial situational awareness products

Initial Response – Sustained Response

During an incident response, BR plays a vital role in ensuring SCE is positioned to address the on-going incident by serving both leadership and support roles.

- Continuously monitor escalation and de-escalation triggers
- Provide corporate-wide situational status/awareness
- Communicate with appropriate internal and external stakeholders
- Support and enhance emergency response capabilities by providing subject matter expertise, and technical knowledge

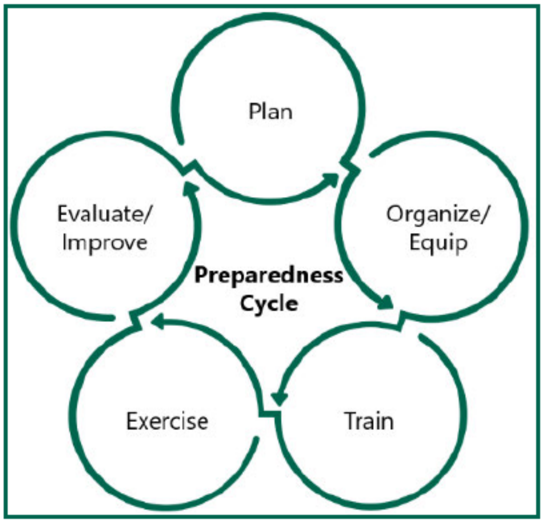
Recovery

As an incident de-escalates and a determination is made to transition from response to recovery, BR plays a critical role in guiding leadership through the transition between phases.

- Right size the current emergency response organization
- Continued coordination with internal and external stakeholders

SCE utilizes the National Incident Management System (NIMS) Preparedness Cycle as a tool to ensure effective coordination during incident response. BR has incorporated the preparedness cycle as part of the emergency response program to prevent, respond to, recover from, and mitigate against natural and human-made disasters.

Figure 3. Preparedness Cycle

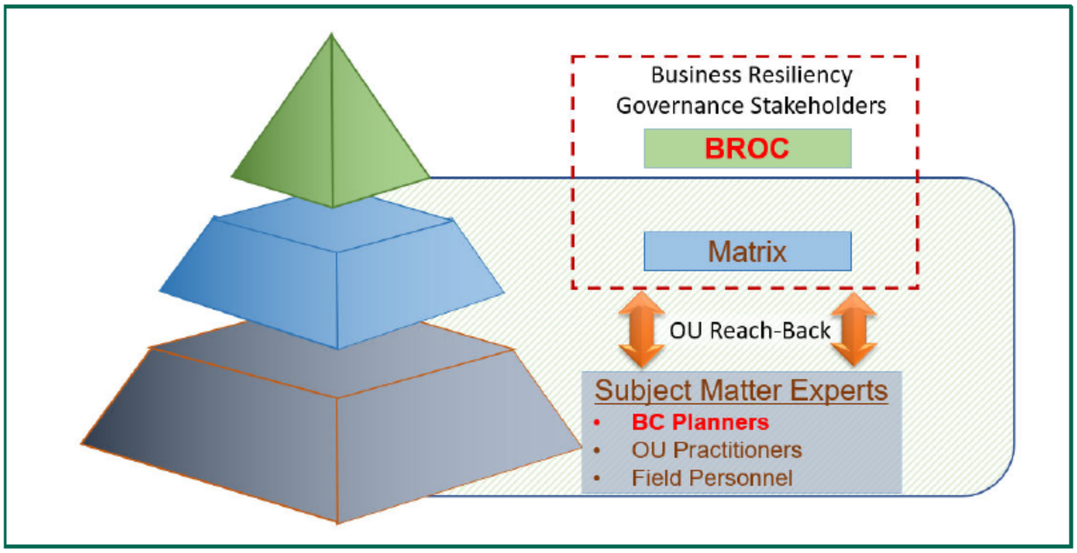


3.2 Business Resiliency Oversight Committee (BROC)

The Business Resiliency Oversight Committee (BROC) is an executive team that provides governance over BR. All decisions must be approved by the BROC.

The BR governance model utilizes a tiered framework to maximize cross component coordination, while ensuring consistency and open communications across OUs.

Figure 4. Governance Structure



3.3 Matrix Stakeholders

A Matrix Stakeholder is a representative from each OUs designed to act as the coordinator between corporate level management and the subject matter experts. A Matrix Stakeholder acts as the conduit between BR and subject matter experts in the OU. Based on the Business Resiliency

Governance Model, all BROC contact must be made through the Matrix Stakeholders since they have the "Reach-Back" capabilities to obtain information.

3.4 Individual Organizational Unit (OU) Roles and Responsibilities

SCE's all-hazards approach is fundamentally rooted in the ability of OUs to execute on core capabilities. Organizational Units prepare for disruptions through a year-round cycle of planning, training, and exercise. OU level responsibilities include:

3.4.1 Planning

Development and maintenance of OU level emergency response and business continuity plans, policies, and procedures.

3.4.2 Training

Ensure OU level personnel meet minimum requirements for individually assigned emergency response role.

3.4.3 Exercise

Participation in the design, development and conduct of emergency response exercises at the OU and Corporate levels.

3.4.4 Emergency Response

Provide OU level resources to assist with emergency response.

- Business Continuity
- Disaster Recovery
- Assessments
- Restoration
- IMT/IST

Organizational Units contribute towards the overall Corporate Emergency Response Organization by providing subject matter expertise during an incident response. OUs participate in a response as part of an IMT, and/or IST.

4 Preparedness

At SCE, preparedness is a fundamental component of the company. Adapting the constructs of the National Preparedness Goal (Prevention, Protection, Mitigation, Response, and Recovery) helps the company organize and identify how each of these efforts contribute to increasing the resiliency of the company and where additional capabilities may need to be built.

4.1 Incident Command System

The Incident Command System is a standardized all-hazards incident management approach that achieves the following:

- Allows the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure
- Enables a coordinated response among jurisdictions and functional agencies, both public and private through IMTs and IST
- Establishes common processes for planning and managing resources, as well as determining and setting objective and priorities

ICS provides an organizational structure for incident management as well as guiding the process for planning, building, and adapting that structure. ICS is flexible and can be implemented for incidents of any type, scope, and complexity. It allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents.

For example, if a disruption is localized to a single business unit, then an IMT may be activated. If a disruption is enterprise-wide, then multiple IMTs may be activated with an IST activating to coordinate the overall response and recovery.

ICS is based on a model adopted by the fire and rescue community and is used by all levels of government—Federal, State, tribal, and local—as well as by many non-governmental organizations and the private sector. ICS is also applicable across disciplines. It is typically structured to facilitate activities in five major functional areas:

- Command
- Operations
- Planning
- Logistics
- Finance/Administration

Note: All the functional areas may or may not be activated based on the needs of the incident.

4.2 Standardized Emergency Management System

The California Standardized Emergency Management System is a structure for coordination between the government and local emergency response organizations. It provides and facilitates the flow of emergency information and resources within and between the organizational levels of field response, local government, operational areas, regions, and state emergency management. SCE has integrated SEMS into its emergency plans and response structure.

During an incident, SCE aligns its response with affected agencies. Coordination with affected agencies requires SCE to engage stakeholders for collaborative planning prior to an incident (i.e., storm, wildfire, PSPS), creating a process to request agency representation during an incident or event, and implementing an IMT structure to manage an incident. SEMS incorporates:

- Incident Command System - A field-level emergency response system based on management by objectives.
- Multi/Inter-agency coordination - Affected agencies working together to coordinate allocations of resources and emergency response activities.
- Mutual Aid - A system for obtaining additional emergency resources from non-affected jurisdictions.
- Operational Area Concept - County and its sub-divisions to coordinate damage information, resource requests and emergency response.

4.3 National Incident Management System

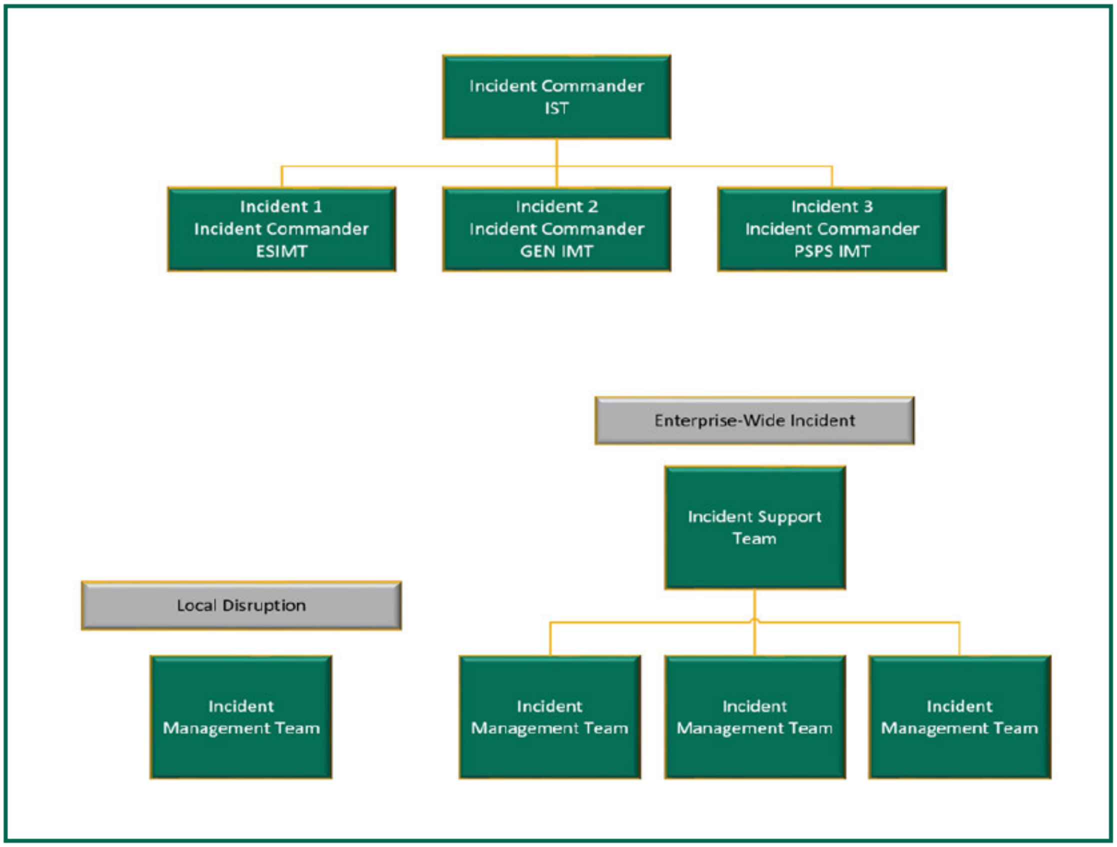
At SCE NIMS provides a consistent framework for incident management, regardless of the cause, size, or complexity of the incident. SCE capitalizes on NIMS by establishing the same foundation for incident management as public sector agencies.

4.3.1 The Incident Management Structure

SCE utilizes the ICS organizational structure to guide its activations, exercises, and its planning process. The flexibility of ICS means it can be adapted for incidents and events of any type, scope, and complexity. It allows its users to adopt an integrated organizational structure that matches the complexities and demands of single or multiple incidents or events.

ICS allows for a scalable response. If a disruption is a localized, single incident in one functional area, only one IMT activates; if multiple incidents occur multiple IMTs may activate as well as an IST to coordinate the overall response and recovery activities and manage resource requirements between the IMTs.

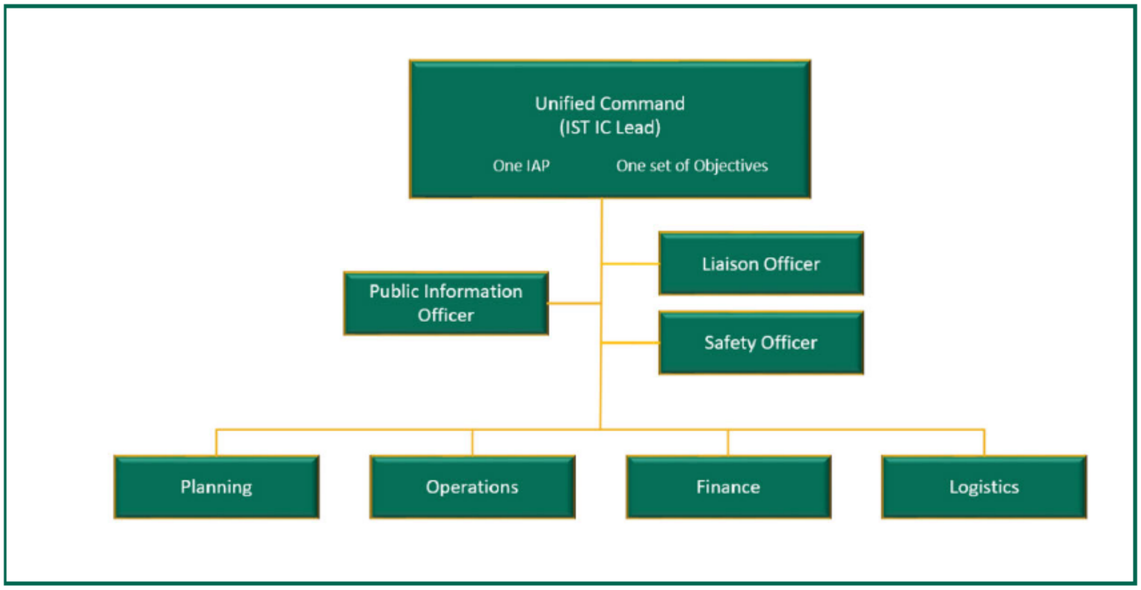
Figure 5. Sample ICS Organizational Structure



4.3.2 Unified Command

A single IMT is typical for situations of limited scope. Additional IMTs and an IST activate for complex incidents with multiple impacts. In the event of a complex incident requiring a response by more than one IMT and coordination of those teams, the individual incident commanders adopt a *Unified Command* structure with all involved IMTs organized into a single team. The IST Incident Commander (IC) leads the unified command effort, and the teams work under a single set of objectives and one incident action plan.

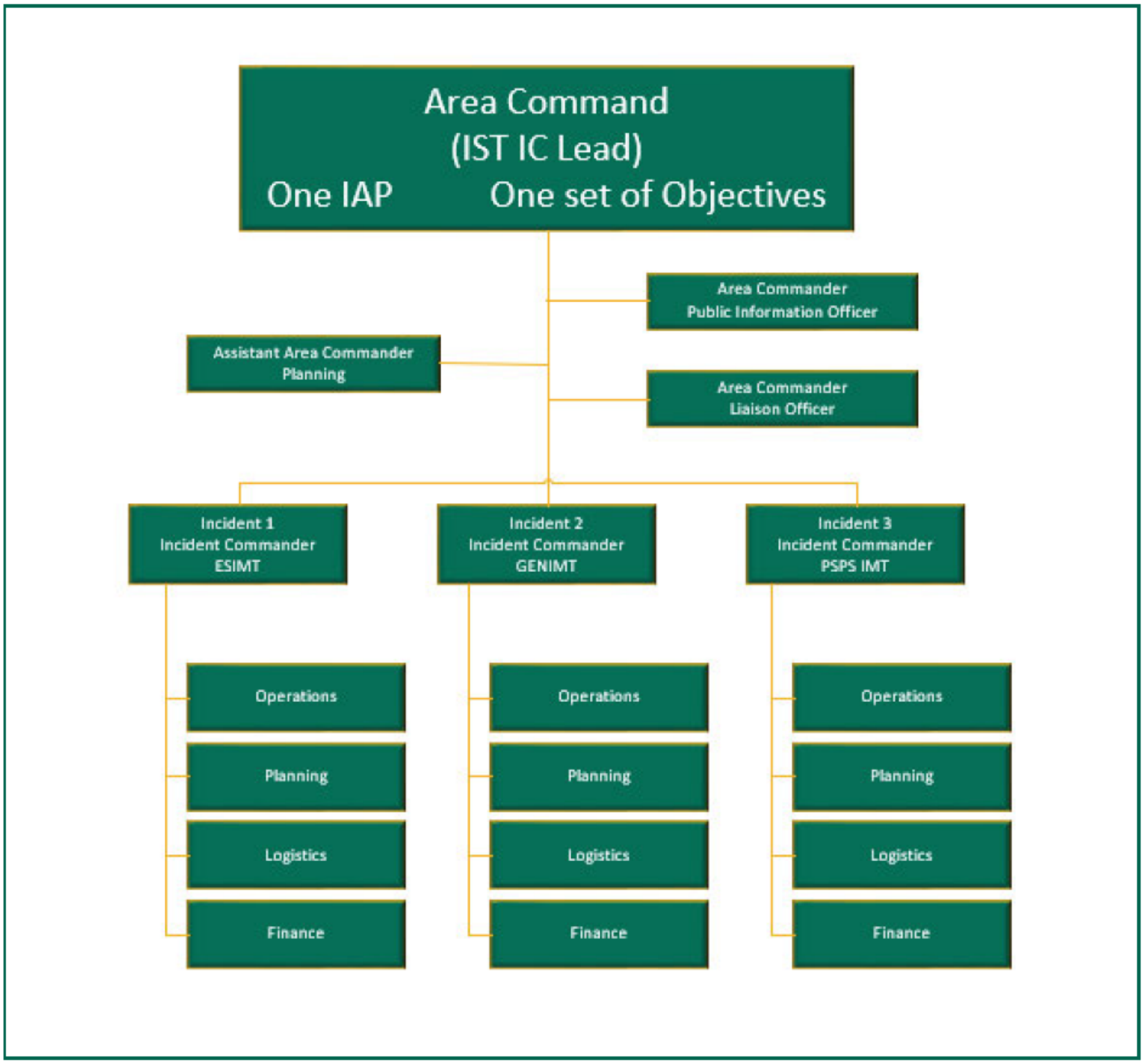
Figure 6. Sample Unified Command Organizational Structure



4.3.3 Area Command

SCE utilizes Area Command as an organizational approach for management of multiple incidents or during large incidents that cross jurisdictional boundaries. Area Command is typical for when an incident calls for a coordinated response, with large-scale coordination necessary at a higher jurisdictional level. SCE will typically organize under Area Command when a single functional business line is affected by multiple incidents across the SCE Service Territory.

Figure 7. Sample Area Command Organizational Structure


Area Command
(IST IC Lead)
One IAP
One set of Objectives
Area Commander Public Information Officer
Assistant Area Commander Planning
Area Commander Liaison Officer
Incident 1 Incident Commander ESIMT
Incident 2 Incident Commander GENIMT
Incident 3 Incident Commander PSPS IMT
Operations
Planning
Logistics
Finance
Operations
Planning
Logistics
Finance
Operations
Planning
Logistics
Finance

4.3.4 Incident Management Teams

SCE established a SEMS, NIMS and ICS compliant incident management structure built around Incident Management Teams (IMTs). An IMT is a group of trained personnel from different SCE organizational units called on to lead a response to an emergency or incident. IMTs typically activate for incidents expected to last longer than a day and requiring coordinated planning and resource allocation within a specific functional area. SCE's primary IMTs are:

- **Electrical Service IMTs** activate when a significant impact to transmission and distribution service has occurred or is imminent. These teams manage tactical resources to achieve objectives set by the Incident Commander to protect, preserve, and restore the system while ensuring the safety of the public and SCE employees.
- **Generation IMTs** activate when an incident occurs or is imminent that interrupts SCE's ability to generate/procure power or involves an SCE generation facility such as generation stations and dams. These teams manage tactical resources to achieve the objectives set by the Incident Commander to generate/procure power, so power production remains consistent during disruptive incidents. The team is responsible for ensuring the safety of the public and SCE employees.
- **Security and Facilities IMTs** activate when an incident occurs or is imminent that causes significant damage, a security breach or threat to any SCE facility and its employees. These teams are responsible for managing resources to achieve the objectives established by the Incident Commander to prevent damage, protect employees and property, and repair facilities. The team is responsible for ensuring the safety of the public and SCE employees.
- **Information Technology IMTs** activate when an incident occurs or is imminent that causes significant damage and disruption to SCE information technology services and systems that could result in a significant operational impact to SCE or have cascading effects of serious magnitude. These teams are responsible for managing resources to achieve the objectives established by the Incident Commander to prevent intrusions and data loss, protect the information technology infrastructure, and recover critical systems. The team is responsible for ensuring the safety of the public and SCE employees.
- **Public Safety Power Shutoff (PSPS) IMTs** activate when conditions are projected to meet established thresholds (combination of fuel conditions and weather). Among many responsibilities, these teams make de-energization decisions, communicate potential outages with public safety partners and customers, manage company notification activities, re-energization activities and notifications. In addition, these teams are responsible for maintaining communications with state/county representatives as required by California State Public Utilities Commission. Subject Matter Experts from across the company can be activated as Technical Specialists to support IMTs. A dedicated PSPS IMT is established to manage the majority of PSPS events with supplemental support from other PSPS IMTs.

4.3.5 Incident Support Teams

The IST oversees the management of a large incident (or multiple simultaneous incidents) that has multiple IMTs assigned. The IST is designed to ensure effective coordination between IMTs, efficient resource allocation and deconfliction, and a single source for messaging. The IST Incident Commander is responsible for the following:

- Establish clear objectives that define the scope of the incident and establish response strategies and priorities
- Ensure a clear understanding of company expectations, intentions, and constraints
- Establish critical resource use priorities between IMTs or groups
- Ensure IMT personnel assignments and organizations are appropriate
- Maintain contact with the CMC and the BR Duty Manager
- Maintain contact with other significant internal and external stakeholders
- Coordinate the demobilization or reassignment of resources
- Facilitate resource support and resource tracking
- Collect, analyze, synthesize, and disseminate information
- Omits the Operations Section Chiefs since the focus is on support and not on operations
- Designed to be used in All Hazards situations and therefore does not specialize in areas such as Electrical Services, IT, or Security

The IST has subtle differences from an IMT due to their overall mission and focus of coordination versus command. Below are a few of the key differences between the IST and an IMT:

- Led by a company officer or executive
- Trained to a higher standard than the IMT members
- Maintains specialty positions on the team that can also be activated to support the IST or IMTs as single resources if necessary. These include:
  - Legal Technical Specialists
  - HR Technical Specialists
  - Environmental Technical Specialists
  - Customer Care Branch Director

4.3.6 Advance Planning Team

The Advance Planning Team (APT) is a cross-functional team that is staffed and assembled on an as needed basis to address a complex and evolving situation that poses a potential safety, operational, economic, reputational, regulatory, or similar risk that could produce cascading impacts, affecting SCE, its employees, or customers. APTs are not intended to make operational decisions or take direct actions to mitigate impacts but should align any engagement strategies and/or communication plans with these activities and coordinate necessary stakeholders to achieve these ends. The APT is designed to address mid to long term issues with potential to cause corporate level impacts and the IMTs are designed to address short-term (immediate) impacts.

4.3.7 Tactical Teams (OU-Level)

Cybersecurity Incident Response Team

The Cybersecurity Incident Response Team (CSIRT) is an Information Technology organizational unit level team responsible for response, containment, and remediation of cybersecurity incidents. During a cybersecurity incident/event CSIRT is responsible for direct investigation and remediation of attacks or compromises to SCE's computing systems.

Business Continuity Teams

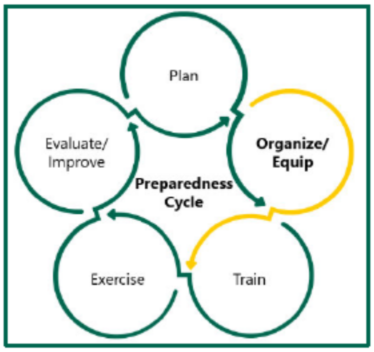
Business Continuity Teams are OU level teams responsible for implementation of business continuity process recovery during a disruptive event.

Disaster Recovery Teams

Disaster Recovery Teams are Information Technology led teams responsible for recovery and restoration of computing hardware, applications, and data.

4.3.8 Crisis Management Council

The Crisis Management Council (CMC) is an oversight committee that provides strategic direction during an incident. The CMC is comprised of five of senior officers (EIX President and CEO, EIX General Counsel, EIXCFO, SCE President & CEO, and EVP of Operations). The senior vice presidents (SVPs) of Corporate Affairs, Regulatory Affairs, Strategy and Corporate Development, Human Resources, Customer Service, Transmission and Distribution, Information Technology/CIO, and VP of Corporate Communications will be activated every time the CMC is activated. Other SVPs and VPs representing organizational units across the company may be activated by the CMC as subject matter experts as needed.



4.4 Mutual Assistance Agreements

Partnership and collaboration between companies to help restore power when internal resources are insufficient. SCE participates in mutual assistance agreements at the State, Regional and National levels.

State-level mutual assistance is requested when SCE identifies resource requirements will exceed existing capabilities. SCE will coordinate with in-state utilities through the California Utilities Emergency Association (CUEA) to request resource needs. CUEA is responsible for facilitating mutual assistance requirements between requesting and responding utilities. CUEA coordinates with the California Office of Emergency Services and staffs the State Operations Center Utility Branch, which allows full coordination between responding organizations.

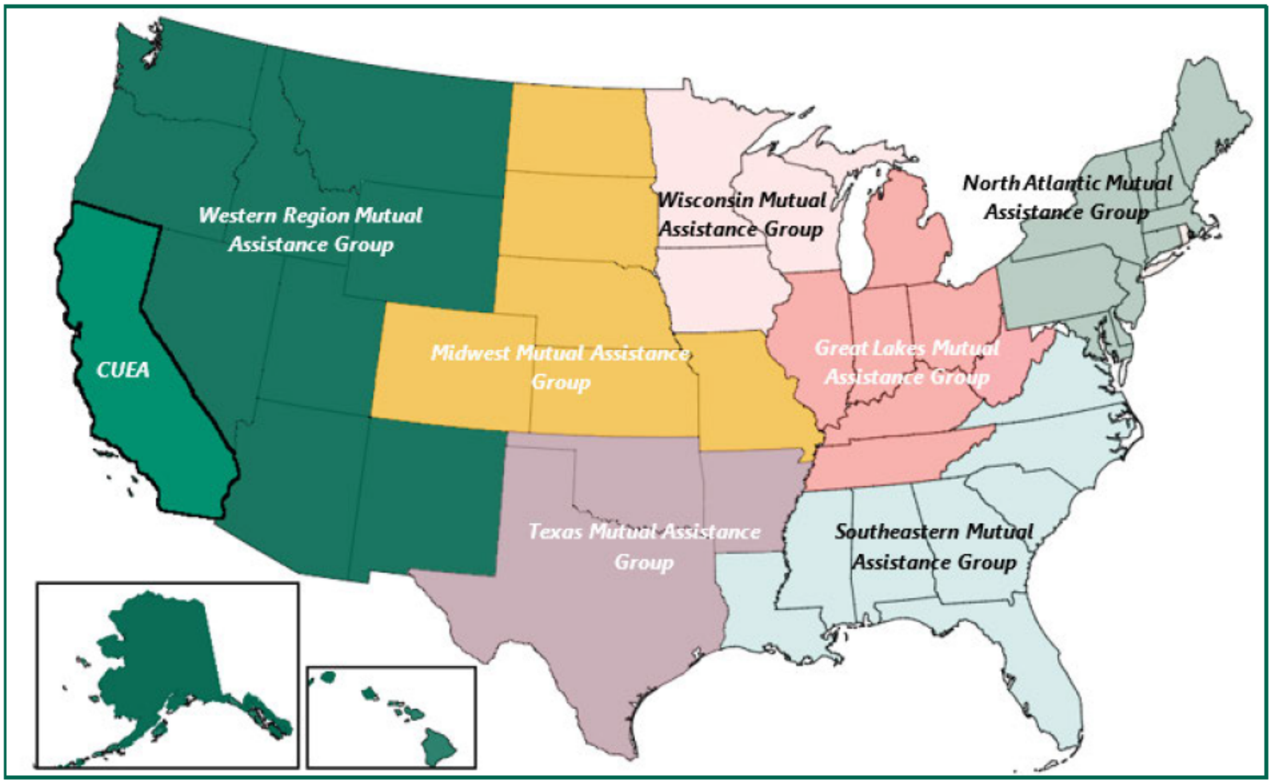
In the event of statewide resource shortfalls, mutual assistance requests are then escalated to the Western Regional Mutual Assistance Group (WRMAG). Similar to CUEA's role at the state-level mutual assistance, the WRMAG facilitates mutual assistance coordination at the regional-level between member utilities.

A National Response Event (NRE) is when a natural or man-made event is forecasted to cause or that causes widespread power outages impacting a significant population or several regions across the United States and requires resources from multiple Regional Mutual Assistance Groups (RMAGs). An NRE declaration is made by the Edison Electric Institute and is reserved only for events that may result in a widespread power outage, such as a major hurricane, earthquake, or an act of war, impacting industry's mutual assistance efforts.

Resources requested through mutual assistance fall under the direct control and authority of the Incident Commander (IC), assigned from the Electrical Services Incident Management Team (ESIMT) for inbound response, and the Resource Planning and Management Manager (RPPM MGR) for outbound response. Assignment of mutual assistance resources are the responsibility of the Operations Section Chief (OSC), Planning Section Chief (PSC), Logistics Section Chief (LSC), Resource Unit Leader (RESL), Mutual Assistance Coordinator (MAC) and Safety Officer (SOF) or the assigned designee.

When restoration objectives are met, resources are released and demobilized back to the coordinating body (CUEA, WRMAG, or NRE pool).

Figure 8. State, Regional, and National Mutual Assistance Designations


Western Region Mutual Assistance Group
CUEA
Midwest Mutual Assistance Group
Wisconsin Mutual Assistance Group
Great Lakes Mutual Assistance Group
North Atlantic Mutual Assistance Group
Texas Mutual Assistance Group
Southeastern Mutual Assistance Group

4.5 Capabilities and Operational Planning

SCE develops and maintains a portfolio of response plans. Response plans developed under steady-state conditions are referred to as deliberate plans which inform decisions, assign tasks, allocate resources, and guide operations during disruptive events. These plans inform Incident Action Plans which are created during an active emergency response.

- All-Hazards Plan
- Crisis Communications Plan
- Crisis Management Council Plan
- Cyber Annex
  - Cyber-Security Incident Response Plan (CSIRP)
  - Ransomware Concept of Operations
- Debris Flow Response Plan
- Earthquake Response Plan
- Electric Emergency Action Plan (EEAP)
- Fatality Incident Response Plan
- Infectious Disease Plan
- North Coast Tactical Plan
- Physical Incident Response Plan

- Restoration Concept of Operations
- Situational Awareness Concept of Operations
- Storm Response Plan
- Wildfire Mitigation Plan

4.6 Tactical Plans

Tactical plans at SCE focus on managing personnel, equipment, and resources that play a direct role in an incident response. Pre-incident tactical planning, based upon existing operational plans, provides the opportunity to pre-identify personnel, equipment, exercise, and training requirements. These gaps can then be filled through various means (e.g., mutual aid, technical assistance, updates to policy, procurement, contingency leasing).

Tactical plans may be developed out of necessity due to avert an incident with the potential for negative consequences or an actual incident requiring specialized capabilities for sustained response and/or recovery.

OU-level tactical plans outline specific procedures to support unique challenges presented by specific incident types. However, OU-Level tactical plans are developed and maintained by Organizational Unit level personnel with support from BR. OUs maintain deployment and redeployment plans for performing safety standby activities and assessing damage during a Major Outage. SCE plans for available personnel to augment responding personnel and in addition, will employ the use of experienced contractors to fill resources needs.

Business Continuity Plans

All SCE Organizational Units develop and maintain Business Continuity Plans (BCPs) to ensure business operations and processes continue even when a disruption occurs. BCPs are part of an annual development process and may be used independently of an IMT/IST activation. If business processes are interrupted when an IMT/IST is activated, the Business Continuity Branch Director will ensure the IST/IMT is informed of business operations and BCP activation. The Business Continuity Branch Director will serve as the coordinator of information back and forth from the OU to the IMT/IST.

Cyber-Security Incident Response Plans

Management of cybersecurity events and incidents is a critical component of SCE’s security program. The Cyber Security Incident Response Plan (CSIRP) offers a methodology designed to minimize operational and business impacts, allow for the expedient return of computing services to normal operations, minimize risks of data loss, and comply with applicable regulations and standards. The CSIRT provides the following:

- Standardizes SCE’s cybersecurity incident response
- Provides insight into cybersecurity threats, risks, and potential impacts

- Improves employee security practices to decrease the risk to SCE's operational and business computing systems

During a cyber related incident typical stakeholder may include:

- Impacted OU BC Teams, impacted system/application DR Team
- BR (BRDM, Watch Office)
- CSIRT
- Information Technology Incident Management Team
- Securities/Facilities Incident Management Team, ESOC
- Incident Support Team
- Crisis Management Council

Disaster Recovery Plans

Disaster Recovery plans are under the general governance and ownership of SCE's Information Technology Department, however Managed Services Providers (MSPs) such as Tata Consulting Services (TCS), and InfoSys maintain and operate critical aspects of the SCE operational and enterprise IT networks, as a result, TCS and InfoSys teams are tasked with ownership of certain disaster recovery plans and processes. TCS and InfoSys DR teams would integrate with SCE IT during a disruptive event and assume roles within the overarching incident, in accordance with ICS principles.

SCE's disaster recovery capability is strongly reinforced through the implementation of ICS (DR Branch within IT IMT Operations Section), and development of incident specific annexes such as the Cyber Security Incident Response Plan and the Ransomware Annex. During an IT related disruptive event, DR and cyber-security plans provide instructions on how to respond and recover, while ICS provides a standardized process for incident organization, reporting, and coordination.

Fatality Incident Response Plan

The Fatality Incident Response Plan (FIRP) outlines how SCE will coordinate a response to any sudden and unexpected employee fatality incident occurring on or off SCE premises, during or after work hours. The SCE FIRP ensures that all members of leadership and responsible entities understand their roles in coordinating an effective response at an enterprise level. The plan is intended to help all individuals involved by clarifying responsibilities and assist with the identification and acquisition of necessary resources. Each person who has a role in this plan must appreciate the critical role that compassion plays in the reduction of suffering and the path toward recovery.

During a fatality incident typical stakeholder could include:

- BR (BRDM, Watch Office)
- Employee's OU leadership
- HR
- CMC

North Coast Tactical Plan

The North Coast Tactical Plan outlines how SCE monitors, prepares for, and responds to a severe winter weather event affecting SCE's North Coast Region. The plan outlines specific tactical procedures to support the North Coast Region considering the unique short-term challenges facing the transmission system and the extensive mitigation efforts that have occurred in the North Coast Region.

Physical Incident Response Plan

The SCE Physical Security Incident Response Plan (PIRP) provides a framework to facilitate an effective response to any size security incident or emergency. The PIRP is a tactical plan, outlining how Corporate Security Operational Leadership will coordinate the initial security response to overcome the unique challenges faced during a physical security incident. This plan ensures key functions are addressed and critical actions are taken following an escalation in the Corporate Security threat condition. During a physical incident typical stakeholder may include:

- BR (BRDM, Watch Office)
- Impacted OU leadership
- Corporate Security leadership
- Information Technology Incident Management Team
- Incident Support Team
- Crisis Management Council
- Securities/Facilities Incident Management Team, ESOC

4.7 Functional Annexes

Functional Annexes to the AHP provide the framework on how SCE executes on functional capabilities such as damage assessment, situational awareness, restoration prioritization, crisis communication, etc. during preparedness, response, and recovery. Functional annexes describe the actions, roles, and responsibilities of key organizations and stakeholders involved with execution of SCE's functional capabilities. SCE's functional annexes include:

- Damage Assessment Concept of Operations
  - The Damage Assessment Concept of Operations outlines the damage assessment process for OUs, Incident Management Team and Incident Support Team after an incident occurs.
- Situational Awareness Concept of Operations
  - The Situational Awareness Concept of Operations provides the framework to build and sustain situational awareness before, during, and after an incident.
- Restoration Prioritization Concept of Operations
  - The Restoration Prioritization Concept of Operations provides the groundwork to ensure that recovery operations of SCE service and assets are initiated during actual or potential incidents.

- Crisis Management Council Plan
  - The Crisis Management Council Plan provides vital information for members of the Crisis Management Council to respond quickly and effectively to a major incident affecting SCE International companies.
- Crisis Communications Strategic Plan
  - The Crisis Communication Strategic Plan is to ensure Edison is positioned to quickly assess potential implications to the company and make key decisions needed to execute a crisis communications plan that facilitates timely, consistent, appropriate and accurate communications to key internal and external stakeholders and maintain the trust and relationship between Edison, its customers, and the community.

4.8 Hazard-Specific Annexes

Hazard-Specific annexes were developed as part of the AHP, to capture strategies in preparation for, response to, and recovery from industry-specific threats and hazards. Content within hazard-specific annexes intentionally focus on special planning needs required for that specific threat/hazard. The contents of these annexes outline SCE's protocols and processes necessary to respond and recover from these hazards and typically include the following:

- Assessment and control of the hazard
- Identification of unique prevention and CIKR protection activities to be undertaken to address the hazard or threat, as appropriate
- Selection of protective actions
- Conduct of public warning
- Implementation of protective actions
- Implementation of short-term stabilization actions
- Implementation of recovery actions.

SCE's Hazard-Specific Annexes include:

- Cyber Annex
  - The Cyber Annex outlines a threat-specific strategy aimed at mitigating, planning for, responding to, and recovering from a cybersecurity incident. The annex is intended as a guide for how SCE will monitor a potential incident, and coordinate critical preparedness, response, and recovery operations including assessing, prioritizing, protecting, and restoring critical IT infrastructure systems or non-publicly available data of SCE during actual or potential cybersecurity incidents (as outlined in the Scenarios and Potential Impacts Matrix) that may have compromised their integrity, confidentiality, or availability.
- Ransomware Concept of Operations
  - The Ransomware Concept of Operations outlines specific processes and actions required to respond to and recover from ransomware incidents, including but not limited to a set of clearly defined roles and responsibilities, organizational structures, communication pathways, and a set of controls for information sharing. Ransomware attacks require a specific set of approaches, processes, coordinating

structures, and incident-related actions for the protection and restoration of the company’s cyber assets, systems, networks, or functions.

- Dam Safety – Emergency Action Plans
  - Dam Safety Emergency Action Plan (EAP) is a document required by California Occupational Safety and Health, and the Federal Energy Regulatory Commission to facilitate and organize employer and employee actions during workplace emergencies.
- Debris Flow Plan
  - The Creek Fire Debris Flow Response Plan addresses how SCE will monitor a potential event and coordinate preparedness, response, and recovery operations in the Creek Fire area – centrally located around Big Creek, CA, in Fresno and Madera Counties, and within the U.S Forest Services.
- Earthquake Response Plan
  - The Earthquake Response Plan (ERP) outlines a strategy for responding to and recovering from a moderate to catastrophic earthquake resulting in significant damage to SCE infrastructure and loss of electrical services to its customers.
- Electrical Emergency Action Plan
  - The Electrical Emergency Action Plan is implemented at the direction of the California Independent System Operator (CAISO) when a statewide or regional imbalance between available system resources and systems demand is imminent or exists. This plan is maintained as mandated by the California Public Utilities Commission (CPUC) and is designed to be used with other operational and response plans.
- Public Safety Power Shutoff (PSPS) Protocol
  - The Public Safety Power Shutoff Protocol describes the procedures and systems used by SCE and the roles and responsibilities of the PSPS IMTs when managing a PSPS event. This protocol describes coordination with public safety partners which is dependent on accurate contact information and regular engagement. BR performs engagements with public safety partners to collaborate on PSPS communication protocols and ensure public safety partner contacts are up to date. A significant part of the PSPS Protocol includes notifications to public safety partners and operational agencies.
  - Access and Functional Needs Plan: Access and Functional Needs population consists of individuals who have developmental or intellectual disabilities, physical disabilities, chronic conditions, injuries, limited English proficiency or who are non-English speaking, older adults, children, people living in institutionalized settings, or those who are low income, homeless or transportation disadvantaged, including, but not limited to, those are dependent on public transit or those who are pregnant.
- Storm Response Plan

  - The Storm Response Plan outlines threat-specific strategy for mitigating, planning for, responding to and recovering from disruptions to the electrical system that cause an outage incident. The purpose of this plan is to guide how SCE will monitor conditions in anticipation of a potential incident and coordinate critical preparedness, response, and restoration activities before, during and after an actual outage incident in the service territory.

- Wildfire Mitigation Plan
  - The Wildfire Mitigation Plan is an adaptive plan developed to reduce the risk of potential wildfire causing ignitions associated with SCE's electrical infrastructure in the High Fire Risk Areas (HFRA) through enhanced system hardening, situational awareness, and operational practices. The plan emphasizes Public Safety Power Shutoff (PSPS) resilience and community engagement while utilizing data, advanced risk analytics and technology to prioritize activities with the greatest potential to mitigate wildfire risks and improve public safety.

4.9 Employee Preparedness

SCE is committed to the safety and welfare of SCE employees and contractors. As part of this commitment, SCE has implemented an employee preparedness program that encapsulates all facets of emergency preparedness. SCE continues to increase employee and family preparedness for catastrophic incidents by providing preparedness information, Emergency Preparedness Checklist, and Response Information or the Emergency Support Locator (ESL), available in the SCE portal.

4.10 Emergency Response Coordinators

SCE Emergency Response Coordinators (ERCs) maintain and administer Emergency Action Plans (EAP) for each SCE facility. SCE ERCs educate and prepares personnel for emergencies and is responsible for the welfare of employees at their respective site. In the event of an incident, ERCs are responsible for the coordination and management of the overall response efforts for a facility.

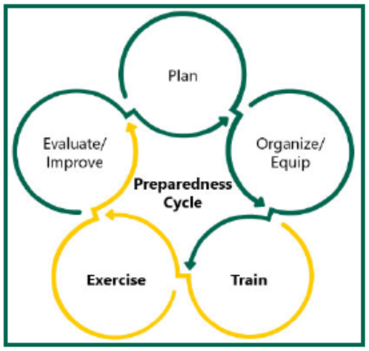
4.11 Life Safety Coordinators

Life Safety Coordinators (LSCs) are SCE employees who assist with emergency preparedness, planning, and response for their work location. LSCs work closely with ERCs to ensure life safety, evacuations, and accountability of fellow employees during an incident. In the event of an incident, LSCs support the ERC by providing direction to occupants assigned to an area to ensure their safety and welfare.

5 Train and Exercise

5.1 IMT/IST Training Program

Initial Qualification Requirements



Team members are required to take on-line training through FEMA's Emergency Management Institute (EMI) & California Specialized Training Institute (CSTI). These independent study courses provide a fundamental understanding of emergency management principles and concepts. While there are several hundred different independent study courses available, SCE only requires the following as prerequisites to classroom training:

- ICS 100.c – Introduction to ICS
- ICS 200.c – ICS for Single Resources & Initial Action
- ICS 700.b – National Incident Management
- IS 800.d - National Response Framework, an Introduction

CSTI certified instructors conduct the classroom training required for IST and IMT qualification. Course materials include activities unique to SCE and the electric utility industry and meet national ICS standards. Some courses include information on SCE-specific plans or technology such as Web EOC.

Team members are required to take *ICS 300 - Intermediate ICS for Expanding Incidents*. **IST Members** must complete ICS 400 after completing ICS 300.

Once training is complete, team members must demonstrate proficiency in their position under the direct supervision of a fully qualified team member during a functional exercise or real-world activation. Collectively, ICS online and classroom training, and exercise/activation components are the minimum qualification requirements needed to build a baseline capability for responding to incidents. Additional familiarity and skill development will continue to take place through formal and informal learning opportunities provided throughout the year.

SCE also requires SEMS G606 online for IMT, IST, Pool Positions and PSPS IMTs personnel

- SEMS G606 - Standardized Emergency Management System Introduction Online Course
- For selected IMT/IST positions SCE will also require G197
  - G197 Integrating Access & Functional Needs into Emergency Management Training

**(Selected IMT/IST positions required to take G197 will be contacted by BR)*

Requalification

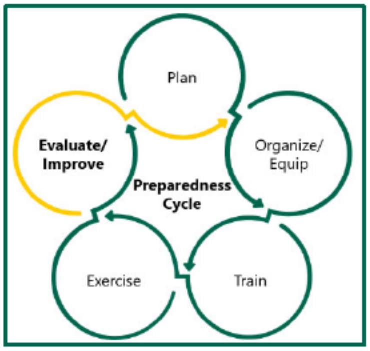
Each year BR requires that all IMT, IST and pooled positions go through requalification to maintain a basic level of familiarity with their position and build on their knowledge, skills, and abilities. BR will annually review qualification requirements and communicate any changes out to all IMT/IST members through the Matrix. To maintain qualification a member must complete the following:

- Positions Specific User Group Training
- IMT/IST Requalification Training

Public Safety Power Shutoff Incident Management Teams, PSPS Task Force and PSPS Dedicated Team **are** required to attend an annual PSPS position specific training and an exercise.

5.2 Homeland Security Exercise and Evaluation Program

The Department of Homeland Security's, Homeland Security Exercise and Evaluation Program (HSEEP) was developed to provide an overview of exercise, development, conduct, evaluation, and improvement planning process. SCE has adapted HSEEP to foster exercise-related interoperability and collaboration. In alignment with HSEEP, SCE identifies gaps and lessons learned from exercises to ensure improvement in the process over time. As part of this improvement process, an Integrated Preparedness Plan is developed to establish a strategy and structure for the exercise program to ensure preparedness efforts are met, while setting the foundation for the planning, conduct, and evaluation of individual exercises.



5.2.1 Exercise Planning

SCE utilizes the HSEEP process to design, develop, conduct, and evaluate SCE specific exercises. HSEEP provides a set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design and development, conduct, and improvement planning.

By incorporating the HSEEP process, SCE develops, executes, and evaluates exercises that address company preparedness priorities. These priorities are informed by hazards, capability assessment findings, corrective actions from previous events, and external requirements. These priorities guide overall direction of an exercise program and the design and development of individual exercises. These priorities also guide planners as they identify exercise objectives and align them to capabilities for evaluation during the exercise.

SCE invites Public Safety Partners to observe and participate in emergency exercises to ensure a high level of coordination and collaboration.

5.2.2 Exercise After Action Reporting and Corrective Action

Following an exercise, After-Action Reports are completed to summarize real world activation and exercises. The AAR provides an analysis of the objectives established during the planning meetings.

Business Resilience assigns and tracks all corrective actions identified during real-world activations and preparedness exercises contribute to the continual improvement of capabilities and inform future planning, training, and exercises. Business Resilience investigates lessons learned from other emergencies affecting utilities and works to implement best practices related to these lessons learned.

5.2.3 Business Continuity Training and Exercises

OU level Business Continuity Plan Managers are responsible for ensuring business continuity teams exercise their business continuity plans in accordance with established policies.

- Each business continuity plan must complete at least a tabletop exercise annually.
- If the business continuity plan contains one or more critical processes, then the plan may participate in a quarterly incident management drills and exercises.
- Select critical processes and plans must participate in the annual SCE full scale exercise (FSE).

5.2.4 Disaster Recovery Training and Exercises

Disaster Recovery Plans are tested to ensure all requirements in the plan can be successfully tested and recovery objectives can be met. Disaster Recovery Testing must ensure the following criterions are met:

- Must be performed annually for all Essential and Critical applications (Recovery Time Objective<24 hours).
- Plans and Runbooks must be developed and maintained for all computing systems/applications regardless of criticality before a computing system is moved into the production environment.
- Must be replaced by quarterly operational failovers, unplanned recovery, or system maintenance where the Disaster Recovery Plan and Runbook is exercised.
- Must be performed prior to implementing a new Computing System in the production environment.
- Must include business involvement and sign off on the recovery environment.
- Include a completed & approved After Action Report (AAR) with recovery evidence.
- The Service Management Operations Organization, infrastructure Service Managers are required to review and sign off all AARs.
- Must be re-tested in the event of an unsuccessful test or when the gap has been corrected, based on a documented project plan.

- Identify and describe the roles and responsibilities for the resources required to meet the recovery objectives and other identified test subjects.
- All identified issues must be tracked until completion.
- Results must be documented.

6 Response

6.1 Concept of Operations

Emergency management during an incident within the SCE Service Territory is a comprehensive effort that requires SCE to work and coordinate with a diverse set of internal and external stakeholders. SCE is be prepared to respond to natural and human-caused emergencies promptly and effectively and to take all appropriate actions including steps to preserve life, and infrastructure, and maintain the ability to deliver safe and reliable electricity.

This Concept of Operations (ConOps) provides further guidance to SCE leadership and emergency responders regarding the sequence and scope of actions to be taken during an incident. It describes all levels of SCE's emergency management capability and corresponding roles and responsibilities; operational procedures during an emergency; and SCE's alignment with SEMS and NIMS. The following concepts also describe SCE's phased approach at emergency response, details functions of the SCE EOC, and demonstrates how information flows internally within SCE and externally to and from various public safety and emergency response partners.

6.2 Emergency Operations Center

Southern California Edison maintains and operates a state-of-the-art Emergency Operations Center (EOC) which includes designated spaces for traditional and alternate communications, operations team, press conferences and other key functions. [redacted]

SCE's EOC is further enhanced by the Watch Office and Situational Awareness Center. The Watch Office and Situational Awareness Center provide 24/7, 365 monitoring and reporting capabilities for the SCE Service Territory. Further enhancements to SCE's capabilities include OU level resources such as:

- Edison Security Operations Center
- Network Operations Center
- Telecomm Control Center

[redacted]

- Grid Security Operations Center
- Generation Control Center
- Grid Control Center

As an additional form of redundancy SCE maintains the ability to conduct virtual operations through the Microsoft Teams platform.

6.2.1 Emergency Operations Center Organization

SCE organizes its EOC following nationally accepted emergency management doctrine (ICS, NIMS) to ensure consistency in approach with other utilities, federal, state, and local emergency management organizations.

SCE's takes on a functional approach towards its Emergency Operations Center Organization. For incidents affecting a single functional area or Organizational Unit, SCE typically activates a functional IMT (Electrical Services, Information Technology, Security/Facilities, Generation) as the primary team responsible for the incident. For incidents affecting multiple functional areas or Organizational Units SCE organizes its Emergency Operations Center under Unified or Area Command. During these instances, SCE activates an Incident Support Team primarily for command and control and functional IMTs to address operational needs of an incident.

During an incident activation, SCE's EOC Organization is primarily responsible for the following:

- **Internal Coordination:** The EOC through Command and General Staff gathers, processes, and disseminates information to internal stakeholders.
- **External Coordination:** The EOC through Command and General Staff provide interface between SCE and public sector emergency management and elected officials. Interface with public sector emergency management and elected officials is primarily conducted through the IST/IMT Liaison Officers and SCE Agency Representatives. As part of external coordination, SCE establishes two-way communication during an incident to share incident status, restoration strategies, and priorities.
- **Resource Management:** The EOC through the Planning and Operations Sections prioritize and allocate incident resources.
- **Safety:** The EOC through the Safety Officer will assure the safety of the public and utility employees. The Safety Officer is responsible to mitigate unsafe conditions, including procedures for Safety Standby.
- **Incident Escalation and De-escalation:** The EOC and Business Resiliency consistently monitor incidents to establish escalation and de-escalation triggers and thresholds.

As a California based utility, SCE also includes portions of the SEMS framework as part of its EOC organizational capabilities, SCE's SEMS participation and alignment includes:

- The Operational Area Concept
- Participation in the Multi-Agency Coordination System (MACS)
- A dedicated EOC

- Personnel on staff who are certified to train on emergency management courses through California Specialized Training Institute (CSTI)

6.2.2 Primary/Alternate EOC Locations

Figure 9. SCE EOC Locations

EOC	Address
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

6.2.3 Mobile Command Centers

SCE's Mobile Command Center (MCC) serves as a readily available, deployable, self-contained resource for use during incident response anywhere in the service territory. The MCC provides response personnel with eight workstations and a small conference room to ensure command, control, and coordination.

6.3 Normal Operations to Activation of the EOC and Resources

SCE operates in a way that allows for movement from everyday normal operations into emergency activation through daily situational awareness and into event specific rapid situational analysis and assessment.

6.3.1 Watch Office Daily Report

The Watch Office Daily Report is an executive summary focusing on information from the previous 24 hours that may influence decisions made by executives or provide a macro view of SCE operations for situational awareness. Watch Office Daily Report contains the following information to inform recipients of the incident status:

- Employee and Public Safety incidents
- New / social media
- Active Incidents
- Electrical System Operations
- Fire Management
- Weather
- Security / Facilities
- Information Technology

Once completed, Critical Incident and Daily Reports are distributed to the following locations:

- All Executives
- Operational Centers including:

[redacted]

[redacted]

- Leadership from:
  - Corporate Communications
  - Local Public Affairs
  - Corporate Storm (T&D Grid Ops)
  - Cybersecurity
  - Claims (Audits, Risk, & Insurance)
  - Customer Contact Center
  - Security
  - Business Resiliency
  - Corporate Safety
  - Customer Service (CSOD, CP&S, BCD)

6.3.2 Activation Process

Within one hour of the identification of a Major Outage, or other emergency response situation, SCE will coordinate internal resources. The following process describes the sequence by which information is gathered, shared, and analyzed between the Watch Office and BRDM, leading up to the decision to activate:

- Watch Office is made aware of an incident
- Incident is reported to the BRDM
- BRDM completes the Complexity Analysis, in consultation with subject matter experts
- Determines incident severity level
- Decides to activate IMT resources*
- BRDM Acts as the Incident Commander until the Command team is fully activated
- The on-duty IC and BRDM work together to determine additional resource need (mobile command center, BR coaches)

Complexity Analysis

When the BRDM receives information that could potentially lead to an activation, an analysis is applied to determine the severity of the incident and how the company should respond. The Complexity Analysis Tool is utilized to provide a standardized and rapid quantitative assessment regarding incident severity level. Severity level determines the course of action when leveraging company resources required to respond and which would be commensurate to the incident complexity.

Complexity Analysis criteria should be reviewed regularly during activations to guide decision making around de-escalation of IMT resources.

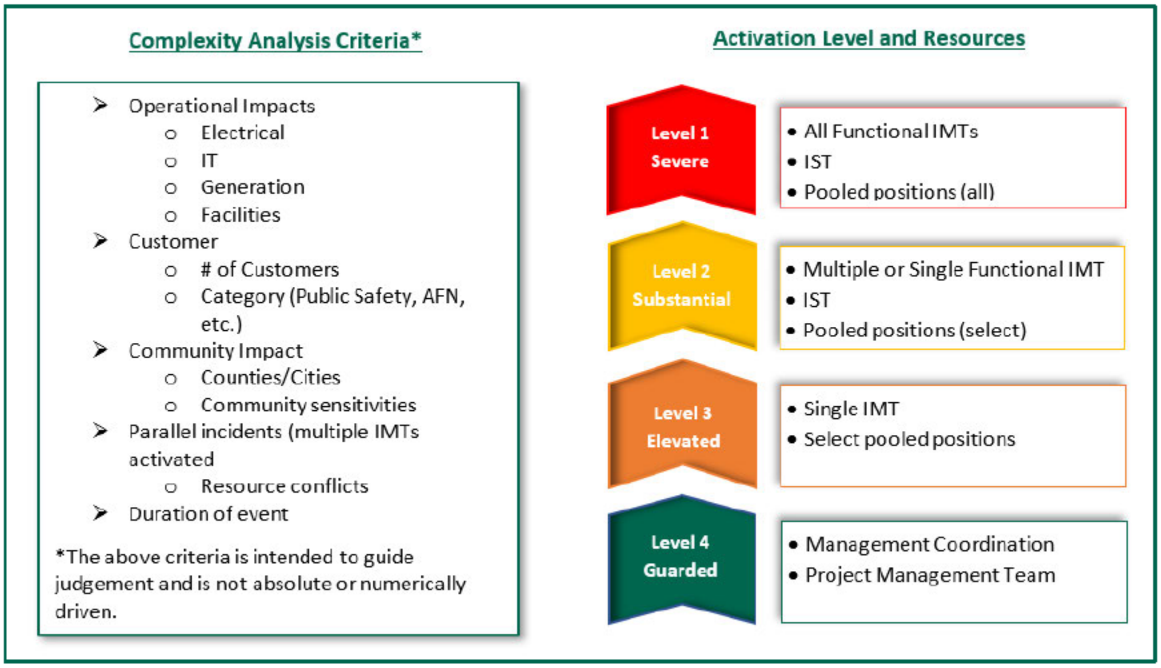
Complexity Analysis Criteria

The criteria in the Complexity Analysis tool is used to determine the severity level of an incident and drives activation decisions for an IMT/IST. The criteria in the Complexity Analysis should be evaluated by the IC and BRDM regularly throughout an activation to assess appropriate staffing levels. This will drive a more gradual and methodical approach to both escalation and de-escalation of resources and ultimately demobilization of an IMT.

Activation Levels

Figure 10 visually depicts SCE's current Activation Levels, and criteria considered and assessed prior to determining the appropriate activation level for an incident.

Figure 10. Complexity, Activation Levels, and Resources



Complexity Analysis Criteria*

- Operational Impacts
  - Electrical
  - IT
  - Generation
  - Facilities
- Customer
  - # of Customers
  - Category (Public Safety, AFN, etc.)
- Community Impact
  - Counties/Cities
  - Community sensitivities
- Parallel incidents (multiple IMTs activated
  - Resource conflicts
- Duration of event

*The above criteria is intended to guide judgement and is not absolute or numerically driven.

Activation Level and Resources

Level 1 Severe	• All Functional IMTs • IST • Pooled positions (all)
Level 2 Substantial	• Multiple or Single Functional IMT • IST • Pooled positions (select)
Level 3 Elevated	• Single IMT • Select pooled positions
Level 4 Guarded	• Management Coordination • Project Management Team

Upon completion of an Incident Complexity Analysis and determination of the activation level, the Officer in Charge (OIC), BRDM and IC will assess for an adequate composition of its EOC Organization and resources necessary for incident response. SCE maintains a roster of qualified Command and General positions who are assigned to the IST, functional IMTs, or as pooled incident resources. Rostered positions establish the foundation of SCE's EOC Organization during any incident response and are further enhanced by non-rostered subject matter experts who are activated to support incidents as needed. When a determination is made to activate non-rostered personnel, these individuals are incorporated into the EOC Organization following traditional ICS/NIMS principles.

6.3.3 Critical Incident Reports

When an Incident Management Team is activated, primary responsibility for maintaining situational awareness of the incident is transitioned from the Watch Office to the Situation Unit Leader on the IMT/IST. Companywide situational reporting for the incident is still the responsibility of the Watch Office.

The Watch Office Critical Incident Report (WO-CIR) are blocks of critical information needed from the incident. Once OU level activities have transitioned to an IMT/IST activation, the WO-CIR provide the onboarding team a better understanding of the current incident status. Reporting criteria for WO-CIRs include:

- Electrical Contact
- IMT/IST Activation
- Security Incidents
- Significant Weather
- Serious Injury
- Significant IT/Telecom Disruptions
- Large, Sustained Electrical Disruptions

6.4 Organizational Unit Coordination

Incident Management Teams at SCE are functionally based and can reach into their respective organizational units during incident response. Organizational unit departments and specialties are incorporated into functional IMTs following ICS/NIMS principles allowing for unity of command, and establishment of a common operating picture.

Transmission and Distribution: The Electrical Services (ES) IMT represents the Transmission and Distribution function of SCE as part of the emergency response organization. The ES IMT coordinates with T&D elements such as District Offices, Distribution Operations Center(s), Switching Center(s), and the Grid Control Center during incident response. All departments within T&D with a role in incident response can be incorporated into the ES IMT organizational structure.

Information Technology: The Information Technology (IT) IMT represents the IT function of SCE as part of the emergency response organization. The IT IMT coordinates with IT elements from Cyber Security, Edison Carrier Solutions, IT Telecom, and IT Grid Services during incident response. All departments within IT with a role in incident response can be incorporated into the IT IMT organizational structure.

Generation: The Generation IMT represents the Generation function of SCE as part of the emergency response organization. The Generation IMT coordinates with Generation elements such as control rooms, Dam Safety, Catalina Island, and Real-Time Trading Desk.

Corporate Real Estate: The Security Facilities (SF) IMT represents the security and facility function of SCE as part of the emergency response organization. The SF IMT coordinates with security and facility elements such as CRE, CBRE (facility vendor), and facility managers.

Corporate Security: Edison Security Operations Center, Regional Security Managers, Insider Risk and Intelligence, Business Operations and Compliance

[redacted]

[redacted]

[redacted]

[redacted]

6.4.1 Functional IMT Indicators

Below are high-level indicators that are evaluated to determine the business case for activating functional IMTs:

Electrical Services IMT

- Customer interruptions
- Isolated damage to transmission or substation facilities within a local region
- Field resources need to be coordinated across impacted area and brought in from other Districts/Regions
- ERTs exceed that of routine isolated incident but aren't expected to exceed 48 hours

IT IMT

- Prolonged failure of critical business applications (Outlook, MS Teams, etc.)
- Active intrusion of Grid or Admin Networks
- Physical security intrusion targeting IT assets (data center or network location)

Generation IMT

- Significant damage or operational disruption of hydro, solar, Peaker or Catalina assets

Security/Facilities IMT

- Emergent threat impacting the safety or security of employees
- Widespread damage to SCE facilities necessitating rapid assessments and restoration
- Targeted attack on company assets
- Other Functional IMT activations that have a security dimension

6.4.2 Resource Scaling

Once initial IMT resources are activated, the Incident Commander, Planning Section Chief and BRDM continue to evaluate any dynamic changes to resource needs which may change throughout the incident.

Objectives: Resource scaling decisions are driven by incident objectives that are developed at the start of an event/incident. They should be re-evaluated daily through the course of the IMT activation to help determine resource needs.

Operational Periods and Shifts: Incident Commanders establish operational periods, the times frames for executing a set of operation actions as specified in the Incident Action Plan. Operational Periods can be of various lengths, although usually not over 24 hours. There may be multiple shifts within an operational period (e.g., 3X 8 hr. shifts or 2X 12 hr.) and shift ranges may vary by position demand and associated deliverables.

6.5 Incident Action Plans (IAPs) and Adaptive Planning

SCE applies standardized incident action planning in accordance with NIMS and ICS. At SCE, the Incident Action Plan (IAP) is central to managing the incident response, the team responsible for managing an incident develops an IAP for each operational period, and the time scheduled for executing a given set of actions as specified in the IAP. The IAP itself identifies the incident objectives and the tactics that will be used to manage the incident during the operational period that the plan was developed for.

The IAPs synchronize operations Companywide and ensures that incident operations are conducted in support of incident objectives. SCE's application of ICS allows for implementation of a disciplined system of planning phases and meetings.

The following objectives for incident management will be incorporated during many emergency responses, especially where a Major Outage or Measured Event is occurring:

- Maintain the safety of customers, employees, contractors, first responders and the general public
- Maintain effective communications with internal and external stakeholders (employees, customers, general public, first responder and emergency management agencies, and public officials) on potential impacts of the storm incident
- Perform safe and timely damage assessment of impacts to electrical infrastructure
- Prioritize restoration activities of electrical infrastructure
- Conduct safe and efficient restoration of critical electric infrastructure
- Monitor conditions within the service territory and the need for potential mitigation activities
- Make attempts to notify customers of potential outages and provide on-going outage updates
- Communicate effectively with internal and external stakeholders (employees, customers, general public, public officials)
- Comply with all identified regulatory requirements
- Consider impacts to the environment

6.6 Field/EOC Communications, Coordination, Direction, and Control Interface

During incident response, communication, coordination, direction, and control between SCE field elements and the EOC follows standardized IMT/IST processes. Often during incident response, field elements are incorporated into the ICS organizational structure as established and determined by the IMT/IST.

Following standard ICS and NIMS principles, SCE integrates affected OUs into the incident organization structure as Branches, Groups or Divisions under the Operations Section. This integration allows for seamless information sharing, command and control, situational awareness, and engagement between all SCE elements involved with incident response. To facilitate coordination and communication with external agencies during times of response, SCE staff may also act as an Agency Representative (AREP), operating as a liaison between SCE's Incident Management teams and the affected communities. AREPs work to identify outages, real and potential issues associated with those outages, and information requests regarding restoration. This relationship allows for increased situational awareness to make informed decisions regarding evacuations, necessary fire-fighting operations and critical restoration times for essential and critical use facilities. SCE also makes every effort to provide space in its Emergency Operations Center for representatives from CalOES, Public Safety Partners, and water and communications infrastructure providers when requested.

SCE utilizes specialized Fire Management staff to monitor, respond to, and report on all fires affecting or having the potential to affect SCE infrastructure. These personnel represent SCE by serving as a Cooperator4 in the field fire incident management structure. Fire Management staff assist in coordinating SCE's response to fires by providing information to manage the bulk electric system, repairing damage, restoring the electric system, and providing safe access to begin restoration work. These personnel maintain close working relationships with fire and emergency management agencies throughout the service territory and serve as consultants and subject matter experts on fire risk management.

On incidents when SCE internal capabilities are overwhelmed, mutual assistance resources are requested and incorporated into the incident organizational structure following the same ICS and NIMS principles for internal SCE resources. At the functional IMT level, the Operations, Planning, Logistics and Finance Sections coordinate with OU level responders to identify mutual assistance needs, internal deployment of mutual assistance resources, work assignments, SCE supervision, field accounting and reconciliation with supporting organization, and logistical support. In the first four hours and throughout the response phase resource requirements will be continually assessed for status and assignment, including the need for Mutual Assistance resources.

6.7 External Agency Coordination and Roles/Responsibilities

6.7.1 Local, State and Federal Command and Control Structure

The responsibility for responding to incidents generally begins at the local level in the city or county affected by the incident. 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 capacity of a local jurisdiction (city or county), local officials contact the state. The Federal Government becomes involved with a response when federal interests are involved; when local and state resources are insufficient and federal assistance is requested; or as authorized or required by statute, regulation, or policy. In some instances, the Federal Government may play a supporting role to local and state authorities by aiding the affected parties. For example, the Federal Government aids local, and state authorities when the President declares a major disaster or emergency under the Stafford Act. In other instances, the Federal Government may play a leading role in the response where the Federal Government has primary jurisdiction or when incidents occur on federal property (e.g., national parks and military bases).

Conceptually, Local, State and Federal agencies integrate during response operations through implementation of NIMS and ICS. Within California SEMS is also applied along with NIMS and ICS and is a fundamental structure for the response phase of emergency management. SCE's SEMS participation and alignment includes:

6.7.2 Public Safety Partners

SCE maintains multiple contacts for each local government potentially impacted by service interruptions. SCE requests that local governments provide a list of officials to be notified (i.e., Public Safety Partners,

[4] A federal, tr bal, state, or local agency that participates with another agency(s) in planning and conducting fire or emergency management projects and activities as defined by the National Wildland Coordination Group (NWCG)

agency management, and elected officials) about service interruptions. SCE performs annual communications test in advance of the peak wildfire season as requested by the Commission and defined by the California Department of Forestry and Fire Protection.

During an EOC activation, SCE ensures public safety partners receive incident related information and timely notifications through the incident Liaison Officer and other SCE designees (Customer Support Branch Director, Regulatory Affairs Technical Specialist) tasked with coordination/notification of public safety partners.

6.7.3 Regulatory Agencies

SCE's Regulatory Affairs has established and maintains points of contact with the CPUC. Business Resilience maintains relationships with Cal OES at the State Warning Center and Cal FIRE. As part of supporting these relationships, SCE regularly updates and shares its contact information (i.e., SCE Watch Office and the Business Resiliency Lead Coach) with County Operational Area representatives. The CPUC Director of Safety & Enforcement Division (SED) is notified of Major Outages, measured events, and PSPS events as soon as it is practical once a decision is made to de-energize. The CPUC SED is also notified within 12 hours after de-energization and upon full restoration within 12 hours from the time the last service is restored.

During an incident SCE regularly communicates with regulatory agencies. Incident communication typically includes:

- Restoration priorities
- Estimates for service restoration

In accordance with CPUC GO166 requirements, SCE within one (1) hour of the identification of a Major Outage, will notify the Commission, affected Essential Customers, and Cal OES Warning Center of the location, possible cause and expected duration of the outage.

- CPUC notification through the website, consistent with ESRB-8, by the Watch Office
- Cal OES Warning Center notification by the BRDM
- Affected area agency representatives will be notified via the same contact lists employed and updated through the PSPS process
    - Automated notification emails sent to Public Safety Partners who have opted in to receive

6.7.4 California Independent System Operator (CAISO) Coordination

SCE through its Electrical Services IMT, via the Grid Control Center (GCC) Real-time desk maintains constant communication with the California Independent System Operator (CAISO) during blue-sky and emergency conditions. The Real-time desk exchanges system status, restoration priorities and status with the CAISO through existing platforms. The CAISO has the responsibility to dispatch available generation assets to meet the electric load requirements of its statewide control area. SCE's internal plans, protocols and procedures work in conjunction with the CAISO's Operating Procedures to achieve a balance between available system resources and system loads when a statewide or regional Operating Reserve deficiency is imminent or exists. SCE will coordinate directly with the CAISO through the Grid Control Center as necessary to manage any emergency incidents, including Major Outages, Measured Events and Storm situations.

6.8 System Operating Bulletins (SOBs)

System Operating Bulletins (SOBs) document the authorities and obligations of the Grid Control Center (GCC) to operate the entirety of SCE's electric system during normal and emergency conditions. During significant events, GCC personnel shall act as the official SCE representative in matters concerning the operation of the SCE electric system.

In the event of a specific hazard, the appropriate System Operating Bulletin (SOB) would be utilized to address system restoration or operating emergencies. The SOBs outline both internal and external communication responsibilities.

6.9 Major Incident Management System (MIMS)

SCE's IT Major Incident Management System (MIMS) is a process which formally classifies Information Technology related incidents. The MIMS process allows IT the ability to identify key stakeholders, determine impact and urgency, and classify priority of an IT incident.

The scope of Incident Management is implemented through a single defined process. Incident Management is mandatory for use by all IT service organizations, technologies, and authorized users. It provides 24/7 support for end user issues, service failures and security incidents.

The Major Incident Management System is a defined process for identifying, recording and resolving Incidents. An Incident is any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to or reduction in the quality of that service.

The primary objective of the MIMS process is to restore services as quickly as possible and to communicate the resolution or workaround to the customer. It also handles queries and requests made by the customers.

6.10 Emergency Management Phases

Figure 13. Emergency Management Phases

Pre-Incident			Response			Recovery
1A	1B	1C	2A	2B	2C	3A
Normal Operations	Increased Likelihood	Credible Threat	Activation	Initial Response	Sustained Response	Long-Term Recovery

6.10.1 Normal Operations

Phase 1A outlines the mitigation and preparedness programs regularly practiced throughout SCE. It is ongoing and informed by hazard assessment and identified mitigation needs to plan, organize, train, equip, exercise, evaluate, and take corrective actions to prepare for an incident.

6.10.2 Increased Likelihood

Outlines the indicators and actions taken leading up to a potential incident, with a focus on gathering initial situational awareness, and ends once the threat has been alleviated or the threat is deemed credible.

The Increased Likelihood phase would only apply to known or anticipated events such as:

- Weather Events (heat, wind, rain)
- Pre-planned Events (PSPS)

6.10.3 Credible Threat

Outlines the advance information and indicators of an event that has the potential to result in a disruption of SCE services and the actions taken immediately before an incident, with a focus on activating personnel and gathering initial situational awareness. The phase ends once an IMT has been activated or the threat has been alleviated.

6.10.4 Activation

SCE utilizes the Emergency Notification System (ENS) platform to communicate with employees during an emergency. ENS is designed to send short messages regarding emergency situations and anticipated actions by personnel via business email, company-issued phones, or work and home voicemail. In addition to communicating with employees, ENS is also the preferred platform at SCE for mobilizing emergency responders. At the onset of an incident, and when a decision is made to mobilize an IST and/or IMT the Watch Office is responsible for initiating ENS to activate a workforce.

Outlines the actions taken during the beginning of a declared incident, with a focus on activating personnel, establishing communications for responders, coordinating information and resources with internal and external partners, and gathering initial situational awareness. Phase 2A ends once Incident Command establishes operational control over the incident, initial safety concerns have been assessed and initial response actions to mitigate the incident have been implemented as appropriate.

6.10.5 Initial Response

Details the actions of the IMT/IST in the early response operation, focusing on situational awareness and establishing a regular response cycle allowing all teams to coordinate effectively. State and federal resources are released based on impact and need. Phase 2B ends when communication between the IMT/IST and field teams is established, a common operating picture has been established, and the requested resources and or information from internal and external partners have been reviewed and support has been requested.

6.10.6 Sustained Response

Outlines the continuing activities of the IMT/IST once operational control, a regular operational cycle, and situational awareness has been established. Any available resources are adjudicated and deployed based on need and impact. Phase 2C ends when response activities set the conditions for long-term recovery, the IMT has been demobilized, and SCE is no longer at risk for continued disruptions due to the incident.

6.10.7 Recovery

Outlines the activities of key personnel following the end of an incident. This includes analysis of an affected infrastructure to determine the potential for hazards, identify indicators to inform mitigation and preemptive measures, and develop a schedule for continued monitoring for post-incident hazards. Phase 3 ends when recovery activities have set the conditions for long-term community recovery and critical facilities and infrastructure are self-sustaining through normal operations.

6.11 Delegation of Authority

During an incident SCE delegates authority from the Crisis Management Council (CMC) Chair to the Incident Commander. The Delegation of Authority typically authorizes an Incident Commander to act on behalf of SCE in the management of response and recovery efforts relating to the incident. The Business Resiliency Duty Manager typically facilitates the delegation of authority process between the CMC Chair and Incident Commander. Listed below are actions that may be delegated to an Incident Commander as directed by the CMC Chair.

- External communication and coordination with senior local, state, and federal representatives
- Communication/coordination with senior regulatory representatives beyond mandatory notifications
- Single expense exceeding $50 million
- Implementation of employee and family support programs
- In-person press conferences
- Board of Directors interaction
- Communication to shareholders and/or the investor community

6.12 Federal and State Support Functions

6.12.1 Emergency Support Functions

Emergency Support Functions (ESFs) are primary disciplines or activities essential to addressing the emergency management needs of communities. ESFs are primarily led by a State or Federal agency, each ESF is designed to bring together discipline-specific stakeholders at all levels of government to collaborate and function withing the four phases of emergency management. SCE and other private sector organizations support multiple ESFs as owners and operators of critical infrastructure.

Figure 14. Federal and State ESFs

Federal ESFs	California ESFs
ESF #1 Transportation	CA-ESF #1 Transportation
ESF #2 Communications	CA-ESF #2 Communications
ESF #3 Public Works and Engineering	CA-ESF #3 Construction and Engineering
ESF #4 Firefighting	CA-ESF #4 Fire and Rescue
ESF #5 Information and Planning	CA-ESF #5 Management
ESF #6 Mass Care, Emergency Assistance, Temporary Housing, and Human Services	CA-ESF #6 Care and Shelter

Federal ESFs	California ESFs
ESF #7 Logistics	CA-ESF #7 Resources
ESF #8 Public Health and Medical Services	CA-ESF #8 Public Health and Medical
ESF #9 Search and Rescue	CA-ESF #9 Search and Rescue
ESF #10 Oil and Hazardous Materials Response	CA-ESF #10 Hazardous Materials
ESF #11 Agriculture and Natural Resources	CA-ESF #11 Food and Agriculture
ESF #12 Energy	CA-ESF #12 Utilities
ESF #13 Public Safety and Security	CA-ESF #13 Law Enforcement
ESF #14 Cross-Sector Business and Infrastructure	CA-ESF #14 Recovery
ESF #15 External Affairs	CA-ESF #15 Public Information
	CA-ESF #17 Volunteers and Donation Management
	CA-ESF #18 Cyber Security

6.12.2 Federal Government Recovery Support Functions

The National Disaster Recovery Framework introduces six Recovery Support Functions (RSF) that are led by designated federal coordinating agencies at the national level. RSFs involve partners in the local, state and tribal governments and private and nonprofit sectors. The processes used for facilitating recovery are more flexible, context based and collaborative in approach than the task-oriented approach used during the response phase of an incident.

Recovery processes are scalable and based on demonstrated recovery needs. Each RSF has a designated coordinating agency along with primary agencies and supporting organizations with programs relevant to the functional area. The RSF Coordinating Agency, with the assistance of the Federal Emergency Management Agency, provides leadership, coordination, and oversight for that RSF. When coordinating agencies are activated to lead an RSF, primary agencies and supporting organizations are expected to be responsive to the function related communication and coordination needs.

The Infrastructure Systems RSF works to efficiently facilitate the restoration of infrastructure systems and services to support a viable, sustainable community and improves resilience to and protection from future hazards. During an event with long term recovery implications, SCE would be expected to support and coordinate with the Infrastructure Systems RSF. Activities related to the Infrastructure Systems RSF would include:

- Participation in planning at all levels.
- Provide technical assistance to all levels of governments for identifying/prioritizing critical infrastructure systems and assets.
- Participation in an inter-agency, inter-jurisdictional recovery planning process.
- Participation in mitigation opportunities that leverage innovative and green technologies.

6.13 Communications Strategy

SCE employs a PSPS compatible Communications Strategy to provide for effective communications with the public before, during and immediately following Major Outages and emergencies. SCE coordinates with various entities and key stakeholders on education, outreach, and feedback in preparation for emergency events which result in any type of outage. This preparedness extends to overall customer resiliency and while it has initially been directed to address PSPS, many of the efforts are also broadly applicable to other extended outages or emergencies. Emergency communication response actions are outlined in the IMT Checklists by response phase to ensure the public and our public safety partners are aware and informed. SCE's Watch Office, Incident Commander, Public Information Officer, Liaison Officer, Operations Section Chief, and Customer Care Branch Director all work together to coordinate internal and external facing communication and messaging.

6.13.1 Whole Community Communications

In advance of potential outages that may affect them, SCE informs state agencies, public safety partners, critical infrastructure and facilities providers, and all customers (including populations from the Disabilities and Access and Functional Needs community) through multiple programs and procedures. SCE considers the following definition of disabilities and access, and functional needs is as follows: populations whose members may have additional needs before, during, and after an incident in functional areas, including but not limited to maintaining independence and the ability to perform the activities of daily living, communication, transportation, supervision, and medical care. Individuals in need of additional response assistance may include those who have disabilities; who live in institutionalized settings; who are elderly; who are children; who are from diverse cultures; who have limited English proficiency or are non-English speaking; or who are transportation disadvantaged. As well as the population of people experiencing homelessness.

6.13.2 Emergency Communications

SCE's layered approach to communication avoids exclusive reliance on online strategies. SCE employs the following methods for communication:

- Interactive Voice Response (IVR) and speaking to SCE Energy Advisor through the Customer Contact Center
- Automated notifications
- SCE.com website with Outage Map showing all types of outages
- Community Resource Centers
- Social Media
- Coordination through Public Safety Partners and their notification systems

SCE maintains Community Crew Vehicles (CCVs), which, when appropriately placed, can assist with communication and support to the public. Each CCV unit contains basic materials needed to engage with the community and are deployed to affected communities as appropriate to the situation, with consideration for public and employee safety.

During incident response, the SCE Emergency Operations Center Organization is responsible for ensuring information sharing across all internal and external stakeholders. The EOC typically serves as the interface between SCE, public sector emergency management, regulatory agencies, and elected officials.

6.13.3 Incident Communications Team/One Voice Messaging

One Voice Messaging is managed by the PIO for distribution to external and internal stakeholders. This is inclusive messaging that is led, developed, and managed by the PIO and distributed during a crisis to stakeholders throughout the company to utilize. All One Voice messaging developed by the PIO, in coordination with key members of the Incident Management Team and/or Incident Support team and must be approved by the Incident Commander prior to release.

6.13.4 Talking Points and Media Statements

Talking points and media statements are information derived from the One Voice messaging developed by the PIO, designed to be tailored and utilized by a variety of company spokespeople to effectively communicate with their respective stakeholders/audiences using established channels of communications (e.g., social media, phone call briefings, employee intranet, press release, press conference, teleconference, one-on-one interviews with reporters, e-mail or written notification, website content with videos).

Provides for timely media coordination before, during and after a Major Outage, including estimated restoration times and potential safety hazards.

6.13.5 SCE.com

SCE.com is a resource provided by SCE to ensure customers are updated with the most current information regarding the status of electricity. In the event of an incident, the website contains an outage center where pertinent information is provided to the customer as event status, Rotating Outage group Id numbers, and outage maps where customers can access the projected restoration times for their service area. During Public Safety Power Shutoffs, clients and the public can gather current information directly from SCE.com. There are two types of information on this page:

- Dynamic information relating to current notifications, de-energizations, re-energizations and locations of Community Crew Vehicles (CCVs) and Community Resource Centers (CRCs).
- Static information explaining the PSPS process, its necessity, and including links for more information, notification sign-ups, additional languages and FAQs

6.13.6 Public Information Communications

Public Information communications refers to any communications developed and delivered to SCE customers. Public Information communications consists of two (2) separate elements. The first element is communications during an unplanned incident, which is derived from One Voice messaging developed by the PIO, in coordination with the IMT/IST and approved by the Incident Commander and tailored towards SCE customers. The second element are pre-developed, customized information and automated to specific customers, homes, and businesses based on location and utilized for automated messaging for planned events (i.e., PSPS, construction or maintenance).

6.13.7 Critical Care Customers

Critical Care is a subset of customers that are enrolled in SCE's Medical Baseline program. Annually, SCE sends all its customers enrolled in the medical baseline program a letter intended to raise awareness of the benefits of the program with emphasis on power outages, requesting their most current contact information preferences. Messaging includes a call-to-action for customers to update their contact information either by phone or on SCE.com so that important alerts and notifications can be sent successfully to them when needed. Knowing that outages can impact customers at any time, this campaign also reminds customers of the importance of having an emergency plan in place for when power outages occur so they can remain resilient during all types of outages. The campaign highlights the critical need for having a plan to power their electrically operated medical or mobility devices during these events. The campaign also includes localized resources that support building an emergency plan.

6.13.8 Critical Facilities and Infrastructure

SCE engages with public safety partners to identify critical facilities and infrastructure that may be impacted by potential outages, as outlined in the CPUC guidance, and other facilities that our public safety partners identify as important. Business Customer Division (BCD) continually assesses the customer contact information for all critical infrastructure and facilities by regularly reaching out to these customers by phone and email, and actively working to update any missing or inaccurate contact information. SCE annually sends its Critical Infrastructure customers an update on its Wildfire and PSPS programs and requests for them to update their customer contact information. SCE also conducts annual Critical Infrastructure workshops where customers provided an overview of PSPS and how to be prepared to be resilient during a PSPS event. SCE on a quarterly basis conducts working group and advisory board workshops where lessons learned between impacted communities and SCE are discussed. Conduct Outreach during this formal environment to the impacted communities to plan the coordination of future de-energization events.

6.13.9 All Other Customers

- SCE ensures that customer contact information is up to date through various sources and channels.
- SCE’s Customer Contact Center procedures include confirmation and updating customer contact information when speaking with our customers.
- SCE.com is enabled with a persistent prompt to remind customers to upgrade their contract information with a link that quickly navigates them to the update page.
- SCE continues community meetings where representatives are available to update customer contact information.
- Requests for customers to update contact information are included on printed material, and bill inserts.
- BCD account managers complete an annual contact certification for all critical infrastructure, government, industrial, and assigned business customers. While this is a normal course of business throughout the year, if update or verification has not occurred, specific outreach is made to ensure contacts are current.
- The request to update information is included in radio spots and media interviews.
- SCE is addressing messages that fail to deliver to a device by removing the incorrect information and verifying the correct information.

6.13.10 Major Outage and Restoration Estimate Communication

Within four **(4) hours of the identification of a Major Outage**, SCE will make information available to customers through our call center and notify Essential Customers, state and local public agencies, and the media of the Major Outage, its location, expected duration and cause (if available). SCE will provide estimates of restoration times as soon as possible following an initial assessment of damage and the establishment of priorities for service restoration.

- SCE's Customer Contact Center is operational 24/7, using restoration information displayed on SCE.com/outages
- SCE's Business Customer Division Outage Management team supports and provide assistance to Business Customers 24/7 with outage related inquiries
- Outage webpage and maps include a restoration estimate in coordination with internal automated status systems
- Estimated Restoration Time is updated after more in-depth assessment, and will be updated throughout the developing situation
- SCE will review restoration estimates for forecast accuracy and address inaccuracies in the forecast restoration estimates
- Macro messaging is used to update website outage page –with broad messaging for regional/complex events
- PIOs can call in directly to DOCs and can also use Pragma Web directly
- SCE will share information with local and tribal governments extend message reach to residents and businesses

Within four **(4) hours of the initial damage assessment** and the establishment of priorities for restoring service, SCE will make estimated restoration times, by geographic area, available through its call center to Essential Customers, state, and local public agencies, and to media. If restoration time estimate is not available, SCE will provide that update.

- IVR & SCE Energy Advisor
- SCE.com Outage Map
- Coordination with Public Safety, local government, and tribal partners

Following a Major Outage, SCE will prepare information for two separate areas:

- **Customer Average Interruption Duration Index (CAIDI)**
  This is a benchmark review of restoration performance, using the Customer Average Interruption Duration Index (CAIDI). CAIDI information will be provided upon request by the Asset, Strategy and Planning Organizational Unit who will fill this request through Integrated System Planning, Special Studies and Reliability, Reliability and Resiliency Senior Manager. The request for CAIDI data will come from the IMT Compliance Unit as documented in the In-Event Checklist. The CAIDI information will be part of the IMT documentation and shared with the Business Resiliency Compliance Advisor for post event reporting.
- **Call Center Performance Data**

A benchmark review of Customer Call Center performance data including the percent of busies calculation and call center metrics will be provided upon request by the Customer Service Organizational Unit who will fill this request through Customer Experience, Marketing and Digital Principal Manager. The request will come from the IMT Compliance Unit. The Call Center information will be part of the IMT documentation and shared with the Business Resiliency Compliance Advisor for post event reporting.

6.13.11 Employee Communications

Employee communications refers to any communications sent to employees. Employee communications are delivered using established internal channels of communication, to include employee emails, the employee portal, talking points for managers, Energized by Edison stories, the Emergency Notification System (ENS), and leadership videos. Employee communications are led and managed by the PIO, with the support of the Corporate Communications team activated as part of an incident response.

6.14 Situational Awareness

A coordinated emergency response relies heavily on comprehensive situational awareness, and the response operations to an emergency event requires the most up to date situational awareness available. Situational awareness encompasses how information is gathered, analyzed, and disseminated to coordinate critical preparedness, response, and recovery operations including assessing, prioritizing, protecting, and restoring critical SCE service and assets during actual or potential incidents.

To achieve situational awareness, information needs must be met for Critical Information Requirements and Essential Elements of Information:

Critical Information Requirements (CIR): Elements of information required by emergency responders and leadership that directly affect decision making. In an emergency response it will be the synthesis of the information being reported out by SCE Organizational Units and the external status information that inform decision making.

- **Essential Elements of Information (EEI)**: Essential Elements of Information (EEIs) frame what information should be collected during an incident and organize the information into reportable categories. EEI is information incident managers need to know to make a timely and informed decision. OUs will be providing EEI when reporting emergency impacts to personnel, equipment, facilities, infrastructure, systems, and technology. The following EEIs provide context and contribute to analysis:
    - Employee accountability including known injuries (source: IST HR Specialist)
    - The status/availability of employees supporting critical processes (source: OUs)
    - Potential hazards that impact the safety and health of SCE personnel and the public
        - Updated common operating picture using modeled data and 'ground truth' information
        - Facility and equipment assessments and operational impacts to SCE
            - Transmission & Distribution
                - Grid Operations (source: GCC and DOCs)

        - Status of the bulk power system
        - Status of the sub transmission system
        - Status of the distribution system
    - Generation
      - Power Supply (source: GOC)
        - Status of SCE generation assets
        - Status of SCE dams
        - Status of connected generation assets
    - Catalina
      - Status of gas, power, water
  - Communications (source: Telecom Control Center)
    - Operational
      - Status of EMS & fiber / microwave connections
      - Status of 900 MHz Radio Network
    - Administrative
      - Status of internet connectivity
      - Status of VOIP/PAX phone network
      - Status of Verizon cell phone network
    - IT Applications (source: GSOC and IT Major Incident Management)
      - Status of applications supporting critical processes
      - Status of SCE data centers
    - Facilities
      - Status of facilities housing critical and essential processes
- Business status of essential processes
- Status of mutual assistance requests
- Interdependencies between SCE, other utilities (water, gas, and electric), government agencies, and critical infrastructure
  - Limitations on transportation due to roadway damage and debris
  - SCE staff supporting external agencies such as JICs, EOCs, and other utilities
  - Ability of government and private sector organizations to continue essential functions
  - Resource shortfalls and supply chain issues
  - The status/availability of employees supporting critical processes
- Business continuity impacts with detail on activation of Business Continuity Plans and status of workarounds

Affected OUs are responsible for collection, management, analysis and reporting of situational status, and for ensuring that relevant information is escalated into or shared with the IMT. Existing tools are available to manage this information, such as Survey 123 or the Collector App, and OUs have the responsibility to develop their internal procedures for effective information collection and transfer to the IMT.

SCE maintains dedicated modeling and analysis tools for All-Hazard and incident-specific threats and hazards. Immediately following an emergency response situation, SCE will begin modeling and analysis to gain a better understanding of potential impacts from the incident. Modeling and analysis results are utilized to inform incident specific next steps such as: mobilization of resources, internal and external coordination, and the composition of SCE's emergency response organization (OU level, and/or EOC).

As SCE progresses from pre-incident into an incident, modeling of known impacts and results from data analysis become essential incident related information. SCE leverages modeling results to inform the deployment of incident resources, establish the geographic boundaries of the incident as it relates to customer impacts, and begin to calculate restoration timelines. The information captured through modeling and analysis is utilized to generate situational awareness documentation for distribution to both internal and external stakeholders.

As SCE moves from Initial to Sustained Response phases of an incident, modeling and analysis activities continue across SCE. At this time the EOC Organization will establish reporting requirements and thresholds for affected OUs, share corporate-wide situational awareness, and coordinate overall response activities. Multiple factors such as availability of resources/personnel, computing, control, and monitoring systems may affect SCE's ability to inform situational awareness and establish a comprehensive common operating picture.

The IMT Planning Section, Situational Awareness Unit will receive modeling information from affected OUs and external sources to produce actionable situational awareness that assists the IMT in timely decision making.

It is the responsibility of the activated IST/IMT to incorporate the findings from modeling and analysis into incident related planning efforts and situational awareness reporting for the duration of the incident. This situational awareness informs decision making including resource coordination and restoration prioritization. It should be assumed that an incident which warrants the involvement of an IST/IMT will include a sizeable situational awareness capability. Coordinating situational awareness will primarily be the responsibility of the IST/IMT Planning Section's Situational Awareness Unit.

Key Sources for Internal Coordination			
Electrical Services	**Generation**	**Security and Facilities**	**Information Technology**
• Grid Control Center • Distribution Operations Center • Field Offices	• Generation Operations Center • Generation Control Centers (Catalina & Big Creek)	• Edison Security Operations Center • Business Continuity Plan Manager(s) • Regional Security Managers	• Grid Security Operations Center • Telecomm Control Center • Service Management Operations Office

In any no-notice event requiring the activation of an IMT/IST, SCE will manage information by established processes according to ICS/SEMS and NIMS.

Initial information and situational awareness will come from multiple platforms/sources are utilized to inform situational awareness, to include:

- Manual processes at the OU Level
- Watch Office
- Situational Awareness Center—including tools such as Seismic IMT Viewer, ShakeCast, GIS, SERA, C-SAV

- Edison Security Operations Center
- Computing systems and/or applications with the ability to inform/alarm operators of real-time conditions

When escalation from normal operations occurs, SCE will begin to consolidate information from both internal and external sources. Internally, SCE gathers information from the same platforms and mechanisms utilized during blue-sky conditions, externally SCE engages with public safety partners, first responder and regulatory agencies to collect information that can assist incident related decision making.

Once an incident occurs, incident related impacts are collected through field observations, automated systems, and communication from affected customers. Information related to the incident gathered at the OU level is then escalated to the Watch Office, and shared with the BRDM, SCE leadership and the in-bound EOC IST/IMT. Situation updates typically originate from affected OUs and then passed to the corresponding IMT Operations Section Branch and shared with the Planning Section's Situational Awareness Unit. Once situation updates reach the Situational Awareness Unit, information is then analyzed, distilled, and shared with incident stakeholders and decision makers. In addition, the Planning Section Documentation Unit is also tasked with ensuring access, storage, and management of incident related information through various existing platforms readily available at SCE. Incident related information is captured and distributed to incident personnel via Incident Action Plans, WebEOC, Critical Incident Reports, Situational Status Reports, and other incident related documents. The information management task will remain the overall responsibility of an IMT/IST's Planning Section for the duration of an incident.

In addition to internal information collection, SCE will likely receive situation reports from local, state, and federal response and regulatory agencies. External situation reports would include key information such as geographic area of impact, agencies involved, current incident status, updates and status of emergency support functions, life safety concerns and priorities, and status of available resources. Aside from formal situation reports from external agencies, SCE gathers incident related information through traditional and social media platforms via Corporate Communications, the Incident Communication Team, and the IMT/IST Public Information Officer.

6.14.1 *Situational Awareness for IMT/IST*

Upon activation, the incoming IMT/IST assumes responsibility for information collection. Multiple Command and General Staff positions are tasked with collecting information from both internal and external stakeholders. Internal information is collected by the Planning Section's Situational Awareness Unit, and the Operations Section's Damage Assessment/Restoration Branch. Once activated, the Restoration Branch will interface with the IMT Operations Section, and affected OUs to coordinate incident operations related to restoration.

External information is collected by the Liaison Officer from partner agencies involved with incident response, and the Incident Communication Team through the PIO collects information from traditional and social media outlets. During incidents with cyber or physical security implications the IT and S/F IMTs would take on the responsibility of coordination with law enforcement and/or intelligence agencies.

During Initial and Sustained Response, the IST/IMT will gather early and detailed damage assessment reports during this phase of the response to begin identifying restoration priorities for the incident. As part of the response operation, the Restoration Branch Director in the Operations Section coordinates with the IST/IMT when collecting damage assessment reports from impacted OUs in the field. Information is collected by the Damage Assessment and Restoration Branch Director, who then shares the information with the Planning Section to process and analyze the data to inform the Restoration Plan.

As the incident progresses SCE begins to establish a common operating picture based on information collected, and begin to inform next steps, such as:

- Incident escalation or de-escalation
- Resource needs
- Restoration prioritization
- Communication strategy

As an incident transitions to Recovery, information collected by SCE would transition from response related elements of information to recovery elements such as restoration timelines, de-escalation efforts, and informing a return to normal operations.

During an incident, external agencies will be working to establish situational awareness. Coordination with external agencies will primarily revolve around the exchange of essential elements of information (EEIs). EEIs can be viewed as incident related information critical for decision making, a public sector agency affected by the same incident could request SCE provide the following:

- Status of electrical system
- # of customers in outage
- Geographical boundaries of impacted area
- Estimated restoration times
- # of critical customers affected

Also, during these incidents, SCE may have an opportunity to receive situational awareness from these same public sector agencies and public safety partners. Types of information the public agencies will be tracking include:

- Geographical boundaries of response area
- Status of roads/transportation impacts
- Status of airports
- Impacts to regional infrastructure
- Communication networks
- Geographic boundaries of impacted area
- Status of debris removal
- Natural Gas and Fuel availability
- Evacuations/shelter locations
- Commodities distribution locations
- Private sector impacts

6.14.2 *Hazard Monitoring*

SCE uses in-house meteorologist staff, data analytics and geospatial tools to create tailored weather service products using field-based weather station information and modeling to inform operational decision-making. When severe weather is forecasted, SCE conducts an evaluation of severity using historical response and management judgment to determine the potential intensity and appropriate response.

6.14.3 Electrical System Monitoring

SCE's Grid Operations is responsible for monitoring and operating SCE's electrical grid in a safe and reliable manner in conjunction with appropriate regulatory agencies. Operating 24 hours per day, 365 days per year, Grid Ops responds first to emergent incidents and monitors situations that might require a significant emergency response. Grid Ops makes the appropriate notifications through the Grid Control Center's notification process as well as notifying the appropriate emergency response personnel whenever a possible or current situation might require a significant response.

6.15 Damage Assessment

Damage assessment is the process for determining the nature and extent of damage resulting in an interruption to SCE services or the loss of critical assets and facilities. The damage assessment process begins immediately following a disruption to services. Damage assessment will begin from the time an OU is made aware of the situation and continues until affected systems, buildings, and infrastructure are restored to steady-state. SCE relies on multiple monitoring and control systems for visibility and operations of the electric grid and supporting infrastructure. These systems are integral to ensuring SCE provides safe and reliable electricity throughout its service area. Having the ability to monitor and control systems through remote means is essential for SCE during both normal operations and emergent situations.

SCE will leverage existing systems (based on availability) to inform an initial diagnosis on system health. Data outputs from monitoring and control systems will provide SCE a baseline understanding of impacts sustained, and immediate next steps. OUs typically mobilize on-hand and on-call resources immediately following an incident. Once mobilized, OU leadership is responsible for organization and deployment of these resources for initial assessments, primary focus areas are as follows:

- Initiate internal early/damage assessment procedures
- Address immediate life safety needs
- Conduct immediate life-safety repairs
- Conduct initial assessments with available personnel and resources
- Identify extent of sustained damages, and inform restoration priorities
- Categorize habitability of facilities
- Inform damage assessment prioritization for area of responsibility

- Document and track results from initial assessments
- Project timeline for assessments

Depending on the scope, size, and severity of an incident, damage assessment can either continue being the responsibility of the affected OU, or the Incident Management Team/Incident Support Team (IMT/IST) emergency response organization may be activated to provide oversight, coordination, and support over an incident with systemwide impacts. In the case of a moderate, severe, or catastrophic emergency event, an IMT will be activated, and damage assessment efforts will inform the IMT/IST for decision making, resource coordination, and restoration prioritization.

Currently, OUs individually assess damage using different methods. Tools available include ArcGIS Survey 123 (accessible to field personnel on mobile devices) and existing OU forms such as CRE's damage assessment forms. CRE uses physical forms to tag each facility and requires the inspector to photograph/scan the forms to the operations center where CRE maintains the results.

For a large-scale response, AirOps collects data and aerial imagery of the geographic location onto a platform known as GeoDVR. The data is then provided to the requesting party and should be shared with the Air Operations Branch Director as well as the Damage Assessment/Restoration Branch Director, for further analysis. It should be noted that LIDAR would be utilized for future damage assessment processes conducted by AirOps.

SCE's Transmission and Distribution (T&D) OU utilizes physical damage assessment tags to mark facilities that have been assessed to minimize the risk of duplicative efforts. Damage assessment activities are coordinated by the T&D Damage Assessment Team and managed through the Outage Management System (OMS) and SAP.

The ATC-20 is a state standard form used to conduct building and safety assessments following an earthquake. These forms are utilized by structural engineers and building inspectors to produce rapid and detailed evaluation reports for post-earthquake damaged buildings. *Refer to Appendix D for samples of ATC-20 Rapid and Detailed Assessment Forms.*

At the onset of damaging impacts to the SCE service area, OUs will utilize existing protocols, and on-hand resources to initiate rapid and immediate damage assessments. OUs responsible for maintenance and operations of key SCE infrastructure usually operate 24x7, 365 days a year. These OUs can dispatch field resources to conduct early assessments and capture damage information, as well as identify disruptions through various real-time control systems. This early information will help to establish the beginning of situational awareness. The OUs will need to ensure timely information reaches the IMT to establish a common operational picture.

As SCE OUs begin to engage in initial assessments, the following criteria will be considered:

- Determine functionality of monitoring and control systems immediately following an incident
- If monitoring and control systems are available, assess the extent of damages/disruptions via information available on these systems

- If monitoring and control systems are unavailable or the data output is not reliable, OUs should plan for conducting manual physical damage/disruption assessments
- On-hand OU supervision should then begin to assemble and organize resources necessary to conduct on-site initial assessments
- OUs will need to establish a regular and timely communication loop with the IMT Operations Section, Damage Assessment/Restoration Branch

The IST/IMT will depend on damage assessment information to inform response operations. It is incumbent upon the OUs to continually update the IST/IMT with updated information as the response continues. Additionally, if ongoing damage occurs throughout the emergency situation, damage assessments may need to be repeated to ensure safety and operational capability of infrastructure, buildings, systems, and equipment.

6.16 Logistics

SCE's logistics capability during incident response is organized under the Logistics Section of an IST/IMT. Following standard NIMS/ICS principles an SCE Logistics Section is led by a section chief, and further organized utilizing Units. Branches and individual contributors filling Technical Specialists roles.

Branch Directors: Support logistics functions under the Logistics Section Chief; Service Branch, Support Branch.

Unit Leaders: Support as functional units under the Logistics Section Chief; Food Unit, Contracts Unit, IT Services Unit, Lodging Unit, Procurement Unit, Laydown Yard Unit.

Technical Specialists: Support logistics functions as an individual contributor/subject matter expert.

6.16.1 Equipment

SCE maintains an inventory of equipment for normal operations and emergent/emergency use. SCE Supply Management is responsible for storage and receipt of goods, movement of materials/equipment, and management of primary equipment vendor contracts during blue-sky and emergency conditions. During incident response, the Logistics Section through the Support Branch, and Contracts Unit will fulfill incident equipment needs.

In addition to Supply Management's inventory of materials and equipment, T&D's Substation Construction and Maintenance manages a stockpile of power transformers, circuit breakers, and disconnect switches through their Emergency Equipment Program.

6.16.2 SCE Emergency Equipment Program

Internally, SCE's Substation Construction and Maintenance organization maintains the SCE Emergency Equipment Program. The Emergency Equipment Program maintains an internal cache of power transformers, circuit breakers, and disconnect switches for emergency use.

6.16.3 Spare Transformer Equipment Program

The Spare Transformer Equipment Program (STEP) is an electric industry program which allows investor-owned, government-owned, or rural electric cooperative electric companies to sell its spare transformers to any other participating company that suffers a "triggering event" defined as an act of terrorism that destroys or disables one or more substations and results in the declared state of emergency by the President of the United States. STEP represents a coordinated approach to increasing the electric power industry's inventory of spare transformers and streamlining the process of transferring those transformers to affected companies in the event of a transmission outage caused by a disruptive event.

6.16.4 SpareConnect

The SpareConnect program provides an additional mechanism for Bulk Power System (BPS) asset owners and operators to network with other SpareConnect participants concerning the possible sharing of transmission and generation step-up (GSU) transformers and related equipment, including bushings, fans, and auxiliary components. SpareConnect establishes a confidential, unified platform for the entire electric industry to communicate equipment needs in the event of an emergency or other non-routine failure.

6.16.5 Staging (Laydown Yard)

SCE utilizes Laydown Yards during both blue-sky and emergency operations for material storage, reporting location for personnel, equipment parking, and field incident command. During an emergency or incident response, The IST/IMT Logistics Section is responsible for:

- Identification of staging/laydown sites
- Set-up, management, and operations
- Coordination between EOC and Staging/Laydown Yard locations

6.17 Restoration Prioritization

SCE begins assessment of restoration priorities and development of a restoration plan once damage assessments results are available and extent of impacts are analyzed. SCE seeks to protect life safety, the environment, infrastructure, and property as base planning factors for restoration planning. Across SCE OUs considerations taken as part of restoration planning include technical factors related to impacts, availability of resources and replacement equipment, as well as internal and external dependencies.

SCE may employ different restoration strategies based on the size, scope, complexity, and intensity of each incident. In smaller, more isolated incidents, SCE typically employs the standard order-based strategy that it uses under routine outage circumstances. As described below, this strategy is not effective in larger incidents where there is an overwhelming volume of orders. When incidents are larger, SCE moves to an area-based strategy where repair priorities are assigned by areas and circuits. This is a tactical decision made during the planning process for a given operational period and documented in the IAP. The two strategy types, order- and area-based can be used together within an event as needed.

6.17.1 Order-Based Strategy

Order based restoration is most frequently applied during less complex incidents where the number of trouble orders is within the capacity of the available workforce to efficiently process and complete.

Order based strategies may also be useful during less complex, distributed incidents where there is not a significant amount of physical damage experienced by the system (e.g., a heat storm). It is also useful before and concurrently with the initial damage assessment before the extent of the damage has been discerned.

The order-based restoration strategy is used when there are a relatively small number of trouble orders. Under this strategy, day-to-day restoration processes predict, locate, and repair faulty equipment or line sections. The Outage Management System (OMS) is used for prioritization of trouble orders based on number of outages and availability of responders.

Order based restoration is very effective when the instances of damage are not substantial and when the number of trouble orders allows efficient work package development and prioritization. The effectiveness of this type of restoration strategy may be diluted when the physical damage is substantial because the time necessary to restore a specific trouble order is not easily incorporated into the analysis, which prioritizes and assigns work. Consequently, during significant incidents where there is widespread damage resulting in numerous trouble orders with physical damage, an area-based restoration strategy may be more appropriate to optimize the restoration effort.

6.17.2 Area-Based Strategy

Area-based restoration strategy is used when the number of orders exceeds the ability to assign work on an individual order basis. Work is assigned to crews by areas or circuits and prioritized at the area or circuit level rather than evaluating individual orders. Areas and circuits are prioritized based on considerations such as customer density and critical restoration issues. Crews are typically expected to complete all the work in their assigned area before moving on to the next. The area-based restoration strategy focuses on de-centralizing the management of significant restoration work to improve productivity while simultaneously addressing high priority issues.

This type of restoration strategy capitalizes on directing multiple resource types, including damage assessors, first responders, company line crews, contract line crews, and mutual assistance resources under one authority, thereby, optimizing their efforts.

6.17.3 Restoration Guidelines

Due to the wide range and nature of incidents, SCE has identified guidelines to restore both the most critical and the largest numbers of customers as quickly as possible while prioritizing public health and safety. With safety of the public and employees as our priority, restoration effort needs to be done in the most efficient manner possible while also maintaining critical infrastructure and reputational considerations. Restoration priority strategy will be based on the following:

- If there is a total or partial system shutdown and subsequent restoration, SCE's priority is to deliver off-site power for bulk power generation start-up. During the process of routing power some

customer load may be restored while energizing bulk power transformers for the coordination of protective relaying equipment, for voltage control, and while picking up station light and power
- Startup power for bulk power generation
- Switching Centers station light and power (if not carried by the emergency generator)
- Offsite power to Diablo and Palo Verde Nuclear Generating Stations if required
- Bulk Power Substations station light and power (if not carried by the emergency generator)
- Customer load

If the total system is not shut down:

- Protect public safety and ensure that utilities and public agencies have electricity
- Repair any facilities that have sustained damage
- Repair transmission lines (66 to 500 kV)
- Ensure substations and circuits are energized
- Repair distribution lines (4 to 66 kV) to restore/maintain service to large numbers of customers
- Repair tap lines to restore service to smaller numbers of customers
- Repair individual customer problems

Some examples of the Restoration Strategy & Priority Order (high to low) are:

- Clear electrical hazard with imminent danger as reported by a public agency
- Clear electrical hazard with imminent danger as reported by the public
- Circuit interruptions
- Unclear electrical hazard with unclear imminent danger as reported by a public agency
- Unclear electrical hazard with unclear imminent danger as reported by the public
- Area Outs
- Single No Lights
- Single Part Lights

6.17.4 Restoration of Critical Assets and Systems

Immediately following a significant disruption to SCE’s service area, the GCC will respond at once to work to create stability in grid operations. The GCC will continue to manage the fluid and dynamic situation with the top priority of grid stability. Restoration of the entire system will require significant coordination and deconfliction of priorities.

Coordinated restoration prioritization begins once damage assessments results are available and the extent of impacts are analyzed. In large incidents, there will be an overlap between restoration prioritization and ongoing damage assessments. The process of restoration prioritization planning includes technical factors related to impacts, availability of resources and replacement equipment, as well as internal and external dependencies. The overall grid stability will be a top priority and will influence the prioritization of Bulk Electric System assets.

Restoration prioritization requires key considerations for the restoration of power following a disruptive event.

- Based on conditions, damaged sections of the electrical system may be de-energized and isolated, allowing service to be restored up to the point of damage, leaving the site safe until permanent repairs can be completed.
- When complete repair is not feasible given the extent of the damage, SCE will either isolate the affected area or provide temporary restoration until repair is possible.
- In wide-spread incidents, SCE assesses and schedules needed repairs to ensure effective utilization of available restoration resources.
- Mutual Assistance Agreements are maintained and activated when the scope of the incident requires additional resources beyond our capabilities.

Restoration prioritization depends upon multiple factors and OU level pre-established thresholds for incident escalation. Considerations for restoration prioritization include:

- Size and scale of the incident
- Availability and adequacy of local resources to conduct assessments
- If there is a total or partial system shutdown and subsequent restoration, SCE's priority is to deliver off-site power for bulk power generation start-up
- Startup power for bulk power generation
- Switching Centers station light and power (if not carried by the emergency generator)
- Offsite power to Diablo and Palo Verde Nuclear Generating Stations, if required
- Bulk Power Substations station light and power (if not carried by the emergency generator)
- Protect public safety and ensure that utilities and public agencies have electricity

Electrical Systems

Prior to initiation of system restoration, a determination must be made if restoration will be conducted under Blackstart or Non-Blackstart conditions. In the case of a total system shut down, and SCE is under Black Start conditions, SCE system restoration will commence by using a managed sub-regional island methodology, [redacted]. In addition, the IMT/IST will provide direct support to the Grid Control Center, by ensuring the availability of Blackstart Units. [redacted].

In the case of partial system shut down, SCE system restoration will commence by adhering to the following concepts:

- Availability and functionality of System Interconnections
- Status of interconnected utility and synchronization points [redacted]
- Access to Lindsey towers

The IST/IMT will be responsible for development of an incident restoration plan, key stakeholders will include:

- Damage Assessment/Restoration Branch Director
- Business Continuity Branch Director
- Advance Planning Unit Leader
- Advanced Planning – Engineering Unit
- Resource Unit Leader
- Operations Section Chief
- Planning Section Chief
- Incident Commander

6.17.5 SCE Infrastructure Prioritization

Restoration prioritization efforts following an incident will be influenced by multiple factors such as:

- Extent of damage sustained along SCE electrical systems, IT systems and applications, and SCE facilities
- Grid stability
- Availability of tie-lines and local generation
- Access to transportation corridors
- Availability of repair parts, emergency inventories
- Integrity of vendor supply chain
- Sufficient personnel for restoration efforts

The IST/IMT will be responsible for the development of the restoration activities during incident response. The emergency response organization will be responsible for the following:

- Identify corporate restoration priorities
- Verify OU level restoration priorities
- Develop Restoration Plan based on restoration priorities
- Conceptually, restoration of SCE's electrical system would begin with restoration of generation assets (internally and/or externally available), transmission lines and substations, then the distribution network. It should be assumed SCE must ensure simultaneous restoration of critical IT systems and applications necessary for safe and reliable delivery of electricity.

Restoration Priority #1: Transmission System

The transmission lines and transmission substations are the highest priority for restoration. Transmission Dispatchers in the Grid Control Center in coordination with the IMT Operations Section Restoration Branch will identify priority transmission lines and substations based on damage assessment results, and criticality of affected lines and substations to development of a restoration strategy.

Restoration Priority #2: Distribution Substations

Concurrent or shortly following restoration of impacted elements of the SCE transmission system, efforts will also focus on restoration of distribution-level substations. When feasible, SCE will partition and isolate damaged portions of the distribution system, and work to identify elements of the distribution system essential to restoration of a sub-regional island, or crank path.

Restoration Priority #3: Distribution Feeders

Restoration of distribution feeders will come shortly following restoration of distribution-level substations. Damaged distribution feeders which support delivery of electricity to critical community infrastructure will be given priority, if operationally feasible. SCE maintains a list of critical community infrastructure for restoration priority. These lists are updated by SCE Account Representatives, in conjunction with county government emergency management staff, and SCE's major and business account services representatives.

Restoration Priority #4: Distribution Laterals

When the feeder system is restored, the fourth priority is restoration of distribution laterals (any single or multiphase electric power line operating at nominal voltage).

Laterals usually are prioritized on a case-by-case basis
The emphasis is to restore the largest number of customers in the shortest possible time
As soon as practicable, crews will transfer de-energized circuits to live circuits or substations

Restoration Priority #5: Individual Service Lines

Service lines will most often be last in priority order for restoration. This will depend on crew availability, location, and other ongoing restoration efforts.

*****Development of a restoration strategy for the SCE electric system will need to consider availability of externally owned and operated generation stations.***

SCE Facilities

There are SCE facilities essential for the operation of the electric system. These facilities include control centers (Grid Control Center, switching centers, Distribution Operations Centers, IT Telecom Operations Center, and Grid Security Operations Center), command centers (Emergency Operations Center, Edison Security Operations Center), data centers. [redacted]

Following an incident, special considerations must be given to SCE's Data Centers due to their critical role in housing applications and data. SCE currently has two data centers. Both data centers work congruently to ensure the seamless storage and transfer of data for SCE. The IMT/IST must establish availability of the following:

Power source – Generators are available on-site once power is lost. The generators utilize combustible diesel fuel and should grid power be unavailable for more than about 5 days (depending on load) then fuel deliveries will be necessary.

Cooling – Since both data centers use water for cooling systems, a steady water supply is needed to ensure the hardware and equipment at the data centers are maintained at the designated temperature.

Critical Personnel – For the data center, these include a mix of SCE personnel and critical vendors. Data Centers are reliant on the external vendor support pre-identified in Business Continuity Plans.

IT Systems and Applications

IT platforms are considered essential for the safe and reliable delivery of electricity. Status of each platform should be established prior to the re-energization of a damaged electric grid. If damage along any of the platforms listed below is experienced, a disaster recovery plan should be implemented and potential work around procedures should be coordinated between IT Disaster Recovery, the Business Continuity Branch Director, and the Damage Assessment/Restoration Branch Director.

For a list of critical IT applications, coordinate with the Business Continuity Branch Director to utilize Business Resiliency Information Management System (BRIMS) to gather data related to critical IT applications.

6.17.6 High Priority Customers

For the restoration prioritization process, SCE has identified customers that provide essential public service as well as critical infrastructure customers who have been pre-identified to be imperative to the broader public safety. Drivers for restoration prioritization consider the following factors:

- Pre-identified essential public service and critical infrastructure customer (hospitals, critical care facilities, police, fire, utilities, food, community support, etc.)
- Length of time without service addresses the outages by criticality further to be addressed as soon as the system has been repaired to support them
- Number of customers affected

SCE will restore facilities so that the greatest number of customers are back in service in the least amount of time. Restoration work is assigned after damage assessment is performed on impacted infrastructure. Once the type of damage and the type of restoration/repair work is known, the appropriate resources are identified and ordered. SCE considers additional priority restoration to the following essential services:

Government Agencies (Municipal)
Government Agencies (National Defense)
Hospitals and Skilled Nursing Facilities
Communication Utilities
Commercial Air and Sea
Electric Utility Facilities and Supporting
Fuel and Fuel Transportation Services
Radio and Television Broadcasting Stations

Water and Sewage Treatment
Areas Served by Networks
Rail Rapid Transit Systems
Customer Served at Transmission Voltages
Optional Binding Mandatory Curtailment Program (OBMC)
Special Exemption Granted by CPUC
Petroleum Refineries

It should be noted that restoration in SCE's service area will shift between outages. As more supply is brought onto the systems, outages may change to ensure grid stability and the effort to restore the greatest number of customers in the least amount of time.

6.17.7 First Responders

A high volume of high priority issues typically occurs at the beginning of a significant incident and often continues throughout the incident. SCE responds to these issues in the order of pre-determined priorities. Personnel are on property throughout SCE territory and on duty 24 hours a day, 365 days a year to respond to these issues. There are qualified personnel throughout SCE who may be called in for additional support. An appropriate number of resources should be reserved to address these critical responses throughout the restoration.

6.17.8 Split Jurisdictions

Substation System Operators manage multiple systems within geographic jurisdictions. In an emergency, the temporary transfer of jurisdiction can be initiated to alleviate the overburdening workloads, thus enabling an impacted Switching Center System Operator(s) to adequately manage the emergency event. This will serve to expedite the restoration of customers while securing public and employee safety and the integrity of the SCE electrical system.

6.17.9 Restoration Complexities

In many emergencies, there are obstacles to swift restoration of service, among those are:

- Vegetation Management: vegetation issues often must be addressed early in the restoration to facilitate the repairs. It is common in an emergency incident to require more vegetation resources than are normally employed on a day-to-day basis. Thus, it is imperative that SCE acquire the adequate vegetation resources and have them on property working as soon as possible. In support of this, SCE has emergency vegetation contracts pre-arranged with both existing vegetation contractors and emergency only, non-standard contractors.
- Total system restoration in a major outage or catastrophic event may be a lengthy process with some service areas experiencing fluctuation in service as grid stability is maintained when additional generation/supply is brought onto the system. Outages may shift as SCE works to restore the greatest number of customers in the least amount of time.

6.18 De-escalation and Demobilization

6.18.1 Transition to Normal Operations or Recovery

Incident de-escalation involves a similar analytical approach to that of incident escalation in the inverse direction. De-escalation is the strategic deactivation or release of positions and assigned personnel. Demobilization criteria is unique to an incident/event and is tied to the incident objectives. As the incident objectives are completed and the incident stabilizes, demobilization will occur. As the need for an IMT/IST diminishes (e.g., rapid decision making, prioritization and allocation of resources), the BRDM and/or BR Managing Director, in consultation with the IC will collaborate with OU leadership to determine the appropriate strategy for transitioning out of the response phase into the long-term recovery phase or normal operations.

IMT/ISTs are designed to address short-term, immediate impacts and after gaining control or mitigating an imminent threat. Command and general staff immediately begin looking at how to transition operations back to normal operations. During every activation, a Demobilization Plan is created that identifies specific demobilization criteria based upon objectives of the Incident Action Plan, allowing for a coordinated, gradual release of resources.

Some large-scale incidents may require extended support beyond initial response of an IMT/IST. In these cases, management of remaining objectives (such as on-going inspections and restoration activities) would be transitioned to blue-sky organizations, Advance Planning Team (APT) or Project Management Organization (PMO).

7 Recovery

Response activities of key personnel will continue until the incident objectives are met as it transitions to the recovery phase. As part of the Recovery phase, analysis of affected infrastructure will determine the potential for hazards, identify indicators to inform mitigation and preemptive measures, and help to establish a schedule for continued monitoring for post-incident hazards. The Response phase ends when recovery activities have set the conditions for long-term community recovery and critical facilities and infrastructure are self-sustaining through normal operations.

7.1 Long-Term Recovery

As incidents de-escalate and stabilize, the focus of activities transitions from initial and/or temporary repairs to long term re-construction of infrastructure deemed irreparable. Planning for and conducting long-term recovery requires unique and specialized skill sets that will differ from resources utilized during incident response. Once the decision is made to transition from response to long term recovery, the Business Resiliency Duty Manager (BRDM), IST/IMT IC(s), and OU level leadership determines the appropriate governance structure responsible for overseeing long-term recovery efforts. Options include devolution of responsibilities to affected OUs, assignment of a Project Management Office, or continued utilization of the Incident Command System through an Advance Planning Team.

7.2 Advance Planning Team (APT)

An Advanced Planning Team (APT) is a cross-functional team assembled to address a complex and evolving situation that poses a potential safety, operational, economic, reputational, regulatory, or similar risk that could produce cascading impacts affecting Edison, its employees, or its customers. APTs are not intended to make operational decisions or take direct actions to mitigate impacts but should align any engagement strategies and/or communication plans with these activities and coordinate necessary stakeholders to achieve these ends.

APTs are activated and directed by the President & CEO of SCE unless the authority is delegated to another member of the leadership team. Coordination of APT activities, including strategic engagement, development of triggers, and other metrics, will be under the direction of the President’s designee and Business Resiliency. The APT will keep senior leadership advised of all significant developments and include a member of the legal team to keep preliminary reports restricted as “attorney-client work product” if necessary.

An APT can operate throughout all phases of emergency management in concurrence with or independent of an IST/IMT, be activated in place of an IMT/IST, or serve as the primary entity once an IST/IMT has been de-mobilized from an incident.

7.2.1 Planning Assumptions

- Typically used in response to planned or anticipated impacts
- Urgent action is needed however there is time to put controls in place and plan for solutions, mitigations, response, and resource needs
- No need emergency measures for spending (use normal protocols)
- The actions of the team are not intended to cause any disruptions or redirection of normal operations.

7.2.2 Process

- Identification of a potential or actual threat/hazard
- BRDM analyzes possible threat and conducts an Incident Complexity Analysis to determine severity level and course of action per routine BRDM escalation protocol
  - **Planned events** (special events, labor issues, scheduled outages)
  - **Emergent events** (irregular weather patterns, pandemics)
- In consultation with Business Resiliency Director, BRDM develops initial objectives, engages stakeholders, and coordinates approach for building team.
- BRDM notifies Officer-In-Charge of anticipated Advance Planning Team activity and intent to update once team structure and objectives are in place.
- Using project management template and develop the following core plan components:

7.2.3 Components of Plan:

- Objectives
- Stakeholders
- Meeting Cadence
- Messaging
- End State Conditions

7.3 ICS (Incident Command System)

Multiple factors such as fulfillment of incident response objectives, and a transition of work assignments from immediate repairs to re-construction of infrastructure inform the transition from Response to Recovery. As response objectives are nearing completion, incident leadership will initiate the development of recovery strategies and objectives.

Incident recovery requires specialized skill sets and expertise which are identified and incorporated into the organizational structure for incident recovery. The BRDM and IST/IMT IC(s) determine the appropriate organizational structure based on the scope, scale, and complexity of restoration/recovery activities. Recovery organizational structures can include:

- Demobilization of non-rostered IST/IMT resources, and/or contract resources
- Demobilization of rostered single resources and/or IST/IMT Sections
- Scaling from Area Command or Unified Command to a single functional IMT

- Turnover from IST/IMT to SCE Organizational Unit(s), Project Management Office, or Advance Planning Team

7.4 Business Continuity Plans (BCP)

SCE requires Organizational Units to develop and maintain BCPs for OU level business processes. Within BCPs, business processes are identified, assigned to process owners, categorized by criticality, and given a recovery time objective. BCPs also include workaround procedures for business process interruptions, OU level roles and responsibilities, as well as integration with the IST/IMT.

- SCE BCPs are typically activated due to the interruption or loss of the following critical resources:
    - Facility Disruption: due to a catastrophic event, or less severe incident negatively affecting business processes.
    - Personnel Disruption: due to a natural disaster, pandemic, or other significant issue resulting in the inability or difficulty for personnel to perform business processes.
    - Technology Disruption: connectivity issues for any period that negatively impacts business processes.
    - Vendor Disruption: for any period that negatively impacts business processes.

Once an interruption to a business process has been confirmed the affected OU assesses severity of the interruption and decides if activation of a BCP is necessary, activation of an OU level BC plan would occur when warranted, with or without the presence of an IST/IMT. Incident complexity and severity determines the size, scope, and configuration of the overall incident response organization. When an incident does not require an IST/IMT activation, the recovery of interrupted processes is the responsibility of the affected OU, and corporate involvement would be limited to information sharing and situational awareness. When an incident requires the leadership and involvement of an IST/IMT, and requires recovery of interrupted business processes, a Business Continuity Branch Director is activated to facilitate coordination between the IST/IMT and OU level Business Continuity Teams.

7.5 Information Technology Disaster Recovery Plans

Disaster Recover refers to the ability to recover computing systems and applications to continue critical functions and business processes after the occurrence or a disaster. SCE's Information Technology Operating Unit develops and maintains specific DR plans for computing systems and applications within the SCE portfolio, these individual plans identify and describe the disaster recovery process to include detailed steps on process recovery, recovery time objectives, tasks and activities, resources and dependencies, and roles and responsibilities for the resources required to meet disaster recovery objectives.

Like OU level Business Continuity Teams, SCE IT has established Disaster Recovery Teams, pre-assigned for recovery of specific computing systems and applications. Once an interruption to a computing system or application has been confirmed, activation of the appropriate IT Disaster Recovery Plan would occur with or without the presence of an IST/IMT. When an incident does not require an IST/IMT activation, recovery of the interrupted computing system or application is the responsibility of the assigned IT Disaster Recovery Team and affected OU. When an incident requires the leadership and involvement of an IST/IMT, and requires recovery of computing systems and applications, a Restoration Branch Director is activated to facilitate coordination between the IST/IMT and IT Disaster Recovery Team(s). In addition to the Restoration Branch Director, IT Disaster Recovery Team(s) would closely coordinate with OU level Business Continuity Teams affected by a loss of technology, and the Business Continuity Branch Director assigned to the IST/IMT.

8 Appendices

8.1 Appendix A: All-Hazards Essential Elements of Information

Essential Elements of Information (EEIs) frame what information is collected during an incident and organizes the information into reportable categories. Information collected through EEIs formulate an incident's common operating picture and contribute towards decision-making. The All-Hazards EEIs provided below serve as a starting point for incident responders and should be modified to reflect specific needs and drive decision-making for individual incidents.

- Employee accountability including reported injuries (source: IST HR Specialist)
- The status/availability of employees supporting critical functions (source: OUs)
- Potential hazards that impact the safety and health of SCE personnel and the public
- Facility and equipment assessments and operational impacts to SCE
    - Power Delivery
        - T&D (source GCC and DOCs)
            - Status of the bulk power system
            - Status of the sub transmission system
            - Status of the distribution system
        - Power Supply (source: GOC)
            - Status of SCE and connected generation assets
            - Status of SCE dams
    - Communications (source: Telecom Control Center)
        - Operational
            - Status of EMS and fiber / microwave connections
            - Status of 900 MHz Radio Network
        - Administrative
            - Status of internet connectivity
            - Status of VOIP/PAX phone network
            - Status of Verizon mobile phone network
    - IT Applications (source: GSOC and IT Major Incident Management)
        - Status of apps supporting critical processes
        - Status of SCE data centers
    - Facilities
        - Status of facilities housing critical and essential processes
- Business status of essential processes
- Status of mutual assistance requests
- Interdependencies between SCE, other utilities (water, gas, and electric), government agencies, and critical infrastructure
- Limitations of transportation due to roadway damage and debris
- SCE staff supporting external agencies such as JICs, EOCs, and other utilities
- Ability of government and private sector organizations to continue essential functions

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	
		[redacted]	
		[redacted]	
		[redacted]	
		[redacted]	

[redacted]

<table>
<tr><th>[redacted]</th><th colspan="2">[redacted]</th><th colspan="2">[redacted]</th><th>[redacted]</th></tr>
<tr><td colspan="6">[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]
[redacted]</td><td colspan="2">[redacted]</td><td>[redacted]</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
</table>

[redacted]

<table>
<tr><td>[redacted]</td><td>[redacted]</td><td colspan="2">[redacted]</td><td>[redacted]</td></tr>
<tr><td colspan="5">[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

8.3 Appendix C: FERC Standards of Conduct

8.3.1 What are FERC Standards of Conduct?

The Federal Energy Regulatory Commission (FERC) Standards of Conduct (SOC) govern the relationship between a transmission provider (SCE) and SCE's affiliated energy marketing functions and require that there be a separation between these two functions. The FERC SOC require SCE to provide non-discriminatory access to transmission service and non-public transmission function information (NPTFI) to all its transmission customers, and without preference to its own affiliated Marketing Function Employees (MFEs). SCE's MFEs are also SCE employees and currently reside in Energy Procurement and Management (EP&M).

8.3.2 What are the normal FERC Standards of Conduct rules?

There are three basic principles to ensure that transmission customers have equal access to non-public transmission system function information. They include:

- *Independent Functioning Rule* – requires transmission function and marketing function employees to operate independently of each other
- *No Conduit Rule* – prohibits passing of non-public transmission function information to MFEs
- *Transparency Rule* – imposes posting requirements to help detect any instances of undue preference due to the improper disclosure of NPTFI

8.3.3 What are some examples of NPTFI?

- Confidential transmission information regarding the scheduling and operation of the transmission system which has not been made publicly available
- Available transmission capacity that has not been made publicly available
- Outage information about specific transmission lines that has not been made publicly available
- Any information regarding short-term, real-time Transmission System Operations that has not been made publicly available.

8.3.4 What is an 'emergency' as it relates to the FERC SOC?

In relation to the FERC SOC, an emergency is considered a scenario where we have a transmission system impact that REQUIRES real-time operations and discussion of NPTFI information in order to recover the system.

8.3.5 When do we request temporary suspension of the FERC SOCs?

The FERC SOC states in part, *"In the event an emergency, such as an earthquake, flood, fire, or hurricane, severely disrupts a transmission provider's normal business operations, the posting requirements in this part may be suspended by the transmission provider. If the disruption lasts longer than one month, the transmission provider must so notify the Commission and may seek a further exemption from the posting requirements."*

Authorized SCE personnel can determine/declare that an emergency situation exists and that adherence to the FERC SOC threatens system reliability.

Examples may include:

- Wildfire that significantly impacts the transmission system
- Catastrophic earthquake
- Cyber-attack impacting the transmission system
- Severe weather resulting in significant transmission system impacts
- Other grid emergency

8.3.6 What does suspension of the FERC SOC allow SCE to do?

After any emergency declaration, SCE employees including those at SCE's Grid Control Center (GCC) or Incident Management Team (IMT) participants have the clearance to disclose NPTFI to MFEs for the purpose of managing SCE's response to the emergency situation.

8.3.7 Process for requesting suspension of FERC SOCs

During an event, SCE can declare an emergency and may suspend the FERC SOC in order to conduct real-time operations and information sharing necessary to recover the system. Emergencies can be declared solely by the GCC or by the Incident Commander (IC) if there is concurrence from the Affiliate Compliance Office (ACO), Law, and the GCC. SCE is unlikely to declare an emergency in a small-scale event; however, we will use discretion based on the specifics of a particular incident when making this determination. For non-GCC SCE personnel that identify a potential emergency situation that may warrant suspension of the FERC SOCs, [redacted] with the ACO for concurrence. Please see below for additional details related to declaring, communicating, documenting, and concluding an emergency.

8.3.8 Identifying Emergency Situation and Declaring an Emergency

An emergency can be identified/declared by the GCC duty manager (or other GCC personnel identified in written procedures) or by an Incident Commander (IC) of an IMT or some other similar cross-department team established to manage a condition that may threaten the transmission system or to maintain system reliability in the face of abnormal conditions.

If an emergency is declared by the GCC, concurrence from the ACO and Law is **not** required.

If an emergency is declared by the IC or other cross-departmental team leader, they must coordinate with SCE's ACO, the Law department, and the GCC prior to such determination.

8.3.9 Communicating Emergency Declaration to Stakeholders

Once it has been determined that an emergency situation exists, the GCC manager on duty, GCC personnel, or IMT lead will then contact other SCE personnel, including MFEs and the ACO regarding the emergency situation in accordance with SCE's internal communication process.

8.3.10 Required Documentation

Response personnel are directed to maintain a record of all NPTFI communications with MFEs and provide this information to the ACO. If feasible, the ACO will review the information and provide additional advice about SOC compliance prior to any disclosure of NPTFI. All disclosures will be posted on SCE's website, www.sce.com, immediately following the conclusion of the emergency situation.

8.3.11 Return to Normal FERC SOC

The emergency shall end when the GCC manager on duty or GCC personnel documents the end of the emergency in the GCC log, or if the emergency was determined by an IMT or other similar cross-department team, when that team, in coordination with the ACO and law department, determines that the emergency situation no longer exists. At the conclusion of the emergency, all impacted SCE personnel will be notified that the emergency has ended and that the FERC SOC posting requirements are no longer suspended.

8.3.12 Tactics to Help Ensure Compliance with FERC SOCs

- Roster non-MFEs to IMTs when possible
- Utilize EPM representatives that are non-MFEs to serve as a liaison between IMTs and MFEs
- Including these guidelines in response plans and incorporate into IMT training

8.3.13 SCE points of contact for FERC SOCs

- [redacted]
    - [redacted]
    - [redacted]

[redacted]

8.4 Acronyms

Acronym	Definition
AAR	After Action Report
AFN	Access and Functional Needs
AHP	All-Hazards Plan
APT	Advance Planning Team
AREP	Agency Representative
BC	Business Continuity
BCP	Business Continuity Plan
BCT	Business Continuity Team
BC Tech Spec	Business Continuity Technical Specialist
BIA	Business Impact Analysis
BPS	Bulk Power System
BR	Business Resiliency
BRDM	Business Resiliency Duty Manager
BRIMS	Business Resiliency Information Management System
BROC	Business Resiliency Oversight Committee
CAISO	California Independent System Operator
Cal OES	California Office of Emergency Services
CCV	Community Crew Vehicle
CMC	Crisis Management Council
ConOps	Concept of Operations
CPUC	California Public Utilities Commission
CRC	Community Resource Center
CRE	Corporate Real Estate
CSIRP	Cyber Security Incident Response Plan
CSTI	California Specialized Training Institute
CUEA	California Utilities Emergency Association
DOC	Distributions Operations Center(s)
DR	Demand Response
DRT	Disaster Recovery Team
EAP	Emergency Action Plan
EEAP	Electric Emergency Action Plan
EIX	Edison International
EMI	Emergency Management Institute
ENS	Emergency Notification System
EOC	Emergency Operations Center
ERC	Emergency Response Coordinator

ERP	Earthquake Response Plan
ESF	Emergency Support Function
ES-IMT	Electrical Services Incident Management Team
ESL	Emergency Support Location
ESOC	Edison Security Operations Center
EVP	Executive Vice President
FAQs	Frequently Asked Questions
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FIRP	Fatality Incident Response Plan
FSE	Full Scale Exercise
GCC	Grid Control Center
GO-166	General Order 166
GCC	Grid Control Center
GSOC	Grid Security Operations Center
GSU	Generation Step-Up
HFRA	High Fire Risk Areas
HSEEP	Homeland Security Exercise and Evaluation Program
IAP	Incident Action Plan
IC	Incident Commander
ICS	Incident Command System
IMT	Incident Management Team
IST	Incident Support Team
IT	Information Technology
IPPW	Integrated Preparedness Planning Workshop
IVR	Interactive Voice Response
JIC	Joint Information Center
LSC	Life Safety Coordinator
LSC	Logistics Section Chief
MAC	Mutual Assistance Coordinator
MCC	Mobile Command Center
MIMS	Major Incident Management System
MSP	Managed Services Provider
NERC	North American Electric Reliability Corporation
NIMS	National Incident Management System
NRE	National Response Event
OIC	Officer in Charge
OSC	Operations Section Chief
OU	Organizational Unit
PAX	PAX Phone
PIO	Public Information Officer
PMO	Project Management Organization
PSC	Planning Section Chief

PSPS	Public Safety Power Shutoff
RESL	Resource Unit Leader
RPPM	Resource Planning & Management Manager
RTO	Recovery Time Objectives
SCE	Southern California Edison
SED	Safety and Enforcement Division
SEMS	Standardized Emergency Management
SOB	System Operation Bulletin
SOC	SmartConnect Operations Center
SOF	Safety Officer
STEP	Spare Transformer Equipment Program
SVP	Senior Vice President
TCC	Telecommunications Control Center
TCS	Tata Consulting Services
T&D	Transmission and Distribution
VoIP	Voice Over Internet Protocol
WECC	Western Electricity Coordinating Council
WO	Watch Office
WO-CIR	Watch Office Critical Incident Reports
WRMAG	Western Regional Mutual Assistance Group

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]