

EnergySec 2026

Tabletop Exercise

Situation Manual

How To Use This Document

This Participant Guide supports active participation in the EnergySec 2026 Tabletop Exercise. It is intended to help participants understand their assigned role, follow the evolving scenario, and contribute to discussion and decision-making. Because the exercise unfolds in stages, participants should use this guide as directed by the facilitator and avoid reading ahead.

Each packet includes information for all ICS roles; however, participants should focus on their assigned position and avoid reviewing information intended for other roles. Role-specific information reflects how real incidents develop, where different teams may receive different facts at different times.

Use this guide as a working reference during discussion. As new updates, injects, or prompts are introduced, consider what is known, what remains unclear, what decisions are needed, and what information should be shared to support a coordinated response.

Participants should approach the exercise with an open, collaborative mindset. The goal is not to test individual performance, but to examine response coordination, situational awareness, escalation processes, communications, and opportunities for improvement.

- **Follow facilitator instructions:** Do not read ahead or review future sections until directed.
- **Stay role-focused:** Use the packet to understand your assigned responsibilities, questions, and concerns.
- **Share relevant information:** Identify what others may need to know to support coordinated decision-making.
- **Think realistically:** If information is incomplete or conflicting, respond as you would during an actual incident.
- **Use the packet as a reference:** Note key facts, impacts, assumptions, and potential follow-up actions.
- **Packet contents include:** scenario recap, role-specific updates, discussion questions, and possible outcome-based information.

Key Objectives for Session

- **Demonstrate tabletop exercise structure:** Walk participants through how a TTX is organized, including scenario introduction, staged injects, role-based discussion, decision points, and facilitated debriefing.
- **Exhibit different facilitation techniques:** Model approaches for prompting discussion, managing time, encouraging quieter participants, redirecting off-topic comments, and drawing out operational insights.
- **Drive participant engagement:** Use realistic scenario details and role-specific questions to encourage active participation, cross-functional communication, and shared problem-solving.
- **Review evaluation practices:** Highlight how observations, participant feedback, strengths, gaps, and improvement opportunities can be captured and translated into actionable after-action items.

Exercise Ground Rules

- **This is a “no fault” exercise:** The purpose is to learn, practice, and identify opportunities for improvement—not to evaluate individual performance or assign blame.
- **Accept the premise of the scenario:** Work within the facts provided, even if some details feel incomplete or artificial, and avoid debating whether the scenario could happen exactly as written.
- **Artificialities exist:** For the purposes of completing the exercise within the allotted time, some information may be presumed or direction given that may seem unrealistic. This is done to progress the exercise and achieve exercise objectives.
- **Use the tools and processes you have available:** Base decisions on existing plans, procedures, systems, communications pathways, and resources that would realistically be available during an incident.
- **Respect each other:** Encourage open discussion, listen actively, allow all roles to contribute, and keep comments constructive and focused on improving the response process.
- **Be honest and realistic:** Share what you think you would actually do, what information you would need, where confusion may exist, and what constraints could affect decision-making.
- **DO NOT LOOK AHEAD IN THE PACKET:** Review only the information released by the facilitator or found in the applicable section of the packet so the exercise unfolds as intended and participants can respond to new information in real time.

Methodology

The Homeland Security Exercise and Evaluation Program, commonly known as HSEEP, is a nationally recognized framework for designing, conducting, evaluating, and improving emergency preparedness exercises. This tabletop exercise uses an HSEEP-informed approach to create a consistent, discussion-based structure that helps participants work through a realistic scenario. This provides a defensible, federally aligned background for exercise development and evaluation. Further, it is being featured in this exercise as a free resource to quickly and easily increase the effectiveness of emergency exercises.

Command Considerations

Questions under the “Command Considerations” are meant to guide your thought process and help you participate in the discussion. They do not need to be answered directly.

STARTEX

Module 1

REMINDER: *Not all of the ICS roles are being activated; only key roles that will drive the scenario.
If you have thoughts to add or concerns that ICS would address outside of your role,
you should still speak up!*

SUN PEAK ENERGY COMPANY PROFILE

Company Overview: Sun Peak Energy is a fictional regional electric utility serving communities across Orange County, California. The company provides electricity distribution, customer account support, outage response, field operations, and grid monitoring services for residential, commercial, municipal, and high-profile destination customers. For the purposes of this tabletop exercise, Sun Peak Energy represents a mid-sized utility with a strong local presence and a customer base that includes critical public venues, tourism destinations, coastal communities, and essential service providers.

Communities and Service Area: Sun Peak Energy serves most of Orange County, including Anaheim and surrounding communities west of Anaheim. Notable customers and service areas include Disneyland Resort, the Anaheim Convention Center, Honda Center, Angel Stadium, nearby state beaches, dense residential neighborhoods, commercial corridors, and hospitality districts that support tourism and regional economic activity.

Office Locations: Sun Peak Energy's primary administrative office and Emergency Operations Center are located just west of Anaheim, California. The company also maintains regional field operations yards and service staging areas positioned throughout Orange County to support outage response, maintenance, dispatch, and customer restoration activities.

Workforce: Sun Peak Energy employs approximately 1,200 staff across office, customer service, field operations, engineering, information technology, cybersecurity, emergency management, safety, finance, and executive leadership functions. Office and field shifts typically conclude around 5:00 p.m., with on-call staffing available to support after-hours incidents, outages, and emergency operations.

Operational Profile: Sun Peak Energy operates customer-facing systems, internal business platforms, field communications, operational technology, and monitoring tools that support reliable electric service. During incidents, the company may activate its Incident Command Structure and coordinate through its Emergency Operations Center to manage service disruptions, cybersecurity concerns, public messaging, employee safety, stakeholder coordination, and restoration priorities.

Key Exercise Relevance: Because Sun Peak Energy serves high-visibility venues, coastal communities, residents, businesses, and public-facing facilities, disruptions can quickly affect customer confidence, public safety messaging, elected officials, media attention, and regional economic activity. The company's dependence on both physical infrastructure and digital systems makes coordinated response across operations, information technology, public information, safety, planning, logistics, and finance essential during a complex incident.

Module 1



Tuesday, August 17, 2026

- 3:00pm
- Weather conditions: Sunny, 75 deg F
- You work for Sun Peak Energy Utility, located just West of Anaheim
- Sun Peak Energy serves most of Orange County, CA
 - Notable areas included in service is Disneyland, Anaheim Convention Center, Honda Center, Angels Stadium, State Beaches
- Customers have been calling in to complain that:
 - Some are losing power
 - Some are having power surges
 - Some are having trouble logging into their accounts online
- Incident Command Structure was activated because of power surges and odd fluctuations in the system.
 - Incident Command is established onsite at Sun Peak's Emergency Operations Center (EOC)

Additional Information

- Other local utilities (water, gas, internet) are not reporting any problems.
- Power teams in the field are not finding any issues with the physical infrastructure that generate or distribute power.
- Office and field shifts end around 5pm.

Module 1 – Scenario Update

- 4:00pm
- IT security team flags **unusual outbound traffic from a network segment connected to operational systems**
- Activity includes:
 - Repeated authentication attempts
 - Data transfer to unfamiliar external IP addresses
- Endpoint detection tools show potential credential compromise
- Neighbor utilities are stating they are not experiencing any issues.



Additional Information

- By this time, executive leadership is taking note, and they are getting calls from Disneyland and Angels Stadium asking about the power fluctuations.
- Elected officials are also getting questions, but are not pushing for information yet.

Decision Point

Option 1	Option 2
Let teams continue working the problem. Need more information to take definitive action <i>Move to page 7</i>	Shut down all physical and digital access to the site. <i>Move to page 9</i>

Module 2

Option 1

Module 2 – Option 1

Tuesday, August 17, 4:30pm

- Disruption is still ongoing
 - Admin/Finance Section has an update
 - Information Technology Unit has an update

Additional Information

- Executive leadership and elected officials and their teams want to sit in on meetings so they have the most up-to-date information.

Decision Point

Option 1	Option 2
Shut down all physical and digital access to the site. Initiate forensic procedures. <i>Move to page 12</i>	Shut down entire network / cease operations. Initiate forensic procedures. <i>Move to page 14</i>

Module 2

Option 2

Module 2 – Option 2

Tuesday, August 17, 4:30pm

- All physical and digital access to the site has been restricted.
 - Staff are sheltering in place
 - All inbound and outbound digital traffic has been temporarily stopped
 - Power still being provided to customers



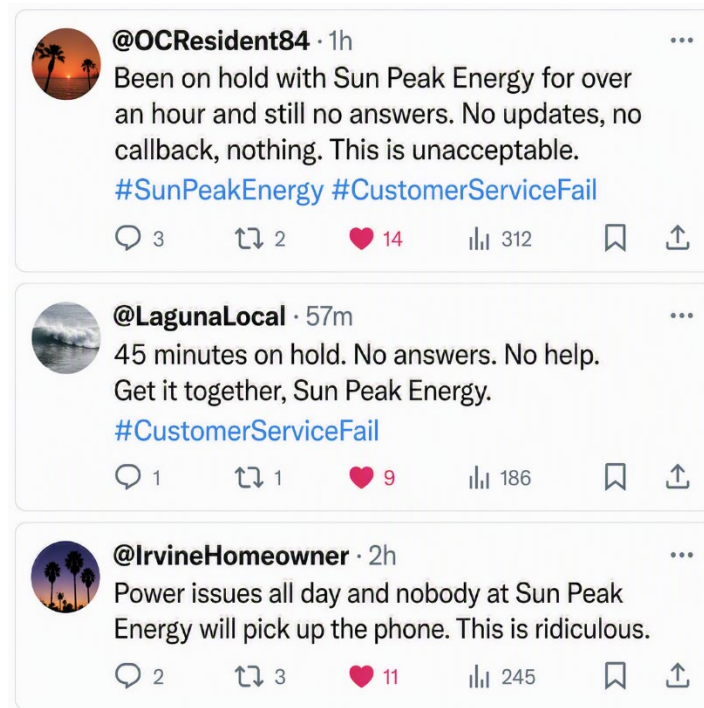
Additional Information

- With stopped inbound/outbound traffic, VPN and all remote access to the systems is suspended
- SunPeak Energy has VOIP phones, which are now also down. People can no longer call via landline to the facility.
- Power is being provided to customers, but a lot of the monitoring infrastructure is down or unable to be accessed.

Module 2, Option 2 – Scenario Update

Tuesday, August 17, 4:45pm

- Social Media is getting a lot of attention
 - People can't call with issues
 - Website is not working
 - They can't pay their bill
- Someone posted a threat of violence on social media because their service is out and they can't contact anyone



Additional Information

- There is no information immediately available about who made the post threatening violence. The only information known is that someone made a threat that is perceived as intending damage to SunPeak Energy facilities and harm to its employees.

Decision Point

Option 1	Option 2
Initiate forensic cybersecurity procedures. (Access still restricted)	Evacuate building and try to service remotely.
Contact Police for support on Workplace Violence incident. <i>Move to page 12</i>	Contact Police for support on Workplace Violence incident. <i>Move to page 14</i>

Module 3

Option 1

Module 3 – Option 1

Tuesday, August 17, 7:30pm

- All physical and digital access remains restricted
 - Staff are still onsite.
- Information Technology Unit Team Leader has an update:



Discussion

Now that the root incident has been resolved, what remaining actions are being considered?

- Restoring access to staff and customers
- Fortifying digital infrastructure

Priorities?

- Restoring access to staff and customers
- Fortifying digital infrastructure

Decision Point

Resolution
Systems have been restarted and are operating normally!
<i>Move to page 16</i>

Module 3

Option 2

Module 3 – Option 2

Tuesday, August 17, 7:30pm

- All physical and digital access remains restricted
 - Staff are evacuated
 - All inbound and outbound digital traffic has been temporarily stopped
- Information Technology Unit Team Leader has an update.

Additional Information:

- All phones are VOIP based, so there is no phone traffic onsite.
- One person from the cybersecurity team needed to stay onsite to do the forensic work because all digital access was cut off.



Discussion

Now that the root incident has been resolved, what remaining actions are being considered?

- Restoring access to staff and customers
- Fortifying digital infrastructure
- Addressing social media furor
- Addressing workplace violence incident

Priorities?

- Restoring access to staff and customers
- Fortifying digital infrastructure

Decision Point

Resolution
Systems have been restarted and are operating normally!
<i>Move to page 16</i>

INDEX

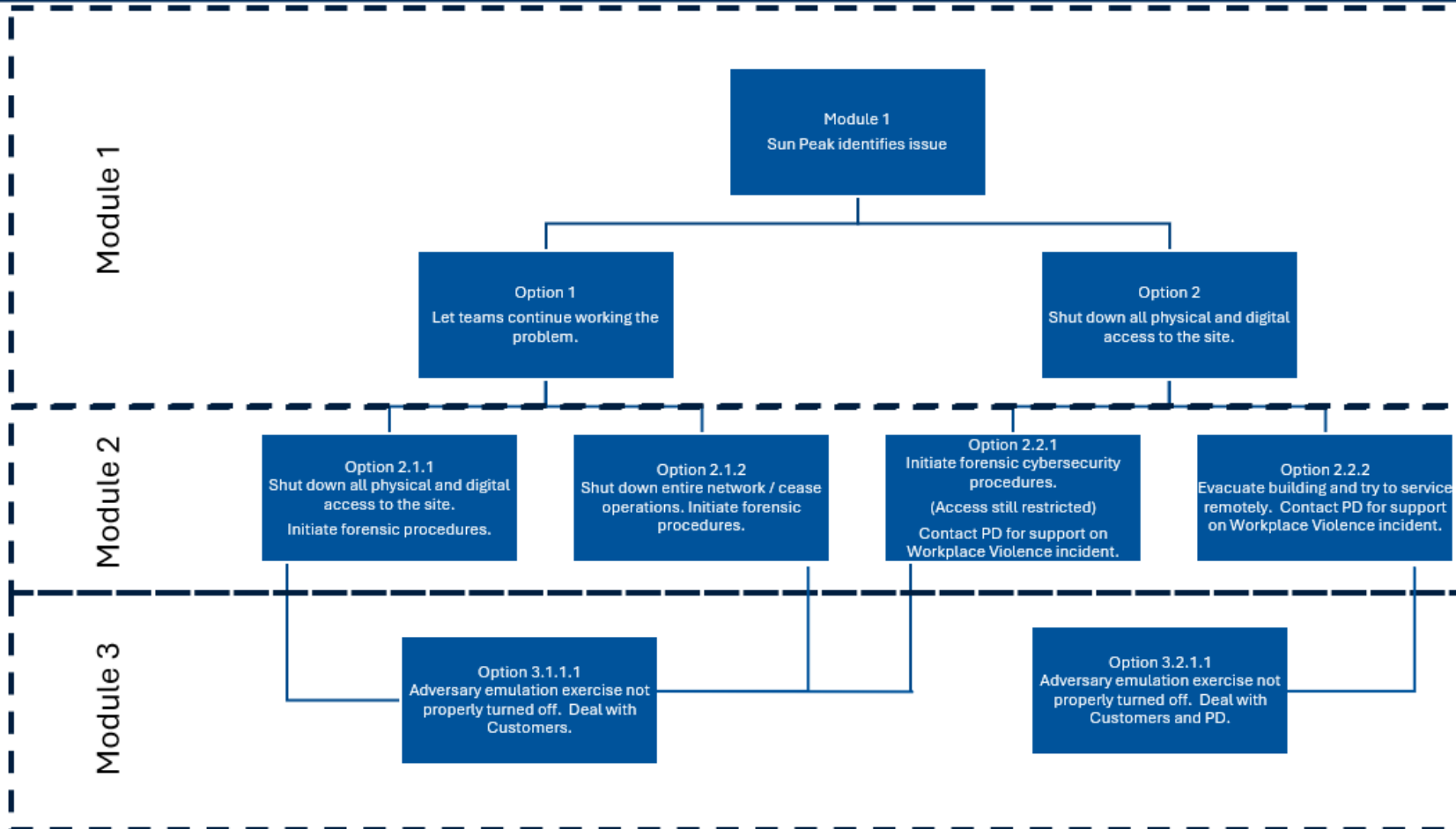
Hot Wash (Exercise)

- What went well?
- What could be improved?
- What did we learn/what was surprising?

Hot Wash (Session)

- Was this a useful conference session?
- What about it was helpful that we should reinforce?
- How can the session be more engaging/insightful?

Exercise Flow/Decision Tree





Participant Feedback Form

Thank you for participating in this exercise.

Your observations, comments, and input are greatly appreciated, and provide invaluable insight that will better allow **EnergySec** to provide engaging and meaningful sessions in the future. Any comments provided will be treated in a sensitive manner and all personal information will remain confidential. Please keep comments concise, specific, and constructive.

Part 1: General Information

Please enter your responses in the form field.

Participant Information
Name (optional):
Agency/Organization Affiliation:
Position Title:
Years of Experience in Present Position:
Location during Exercise:

Please circle the appropriate selection.

Number of Exercises Previously Participated in:	0	1 – 5	6 – 10	11 – 15	16+
--	---	-------	--------	---------	-----

Please circle the appropriate selection.

Exercise Role:	Player	Facilitator/ Controller	Evaluator	Other
-----------------------	--------	-------------------------	-----------	-------

EnergySec 2026

Tabletop Exercise

PARTICIPANT GUIDE

Sun Peak Energy Company Profile

Company Overview: Sun Peak Energy is a fictional regional electric utility serving communities across Orange County, California. The company provides electricity distribution, customer account support, outage response, field operations, and grid monitoring services for residential, commercial, municipal, and high-profile destination customers. For the purposes of this tabletop exercise, Sun Peak Energy represents a mid-sized utility with a strong local presence and a customer base that includes critical public venues, tourism destinations, coastal communities, and essential service providers.

Communities and Service Area: Sun Peak Energy serves most of Orange County, including Anaheim and surrounding communities west of Anaheim. Notable customers and service areas include Disneyland Resort, the Anaheim Convention Center, Honda Center, Angel Stadium, nearby state beaches, dense residential neighborhoods, commercial corridors, and hospitality districts that support tourism and regional economic activity.

Office Locations: Sun Peak Energy's primary administrative office and Emergency Operations Center are located just west of Anaheim, California. The company also maintains regional field operations yards and service staging areas positioned throughout Orange County to support outage response, maintenance, dispatch, and customer restoration activities.

Workforce: Sun Peak Energy employs approximately 1,200 staff across office, customer service, field operations, engineering, information technology, cybersecurity, emergency management, safety, finance, and executive leadership functions. Office and field shifts typically conclude around 5:00 p.m., with on-call staffing available to support after-hours incidents, outages, and emergency operations.

Operational Profile: Sun Peak Energy operates customer-facing systems, internal business platforms, field communications, operational technology, and monitoring tools that support reliable electric service. During incidents, the company may activate its Incident Command Structure and coordinate through its Emergency Operations Center to manage service disruptions, cybersecurity concerns, public messaging, employee safety, stakeholder coordination, and restoration priorities.

Key Exercise Relevance: Because Sun Peak Energy serves high-visibility venues, coastal communities, residents, businesses, and public-facing facilities, disruptions can quickly affect customer confidence, public safety messaging, elected officials, media attention, and regional economic activity. The company's dependence on both physical infrastructure and digital systems makes coordinated response across operations, information technology, public information, safety, planning, logistics, and finance essential during a complex incident.

INCIDENT COMMAND POSITION PROFILES

REMINDER: *Not all of the ICS roles are being activated; only key roles that will drive the scenario.
If you have thoughts to add or concerns that ICS would address outside of your role,
you should still speak up!*

INCIDENT COMMANDER

Position Parameters: The Incident Commander has overall responsibility for managing the incident, setting response objectives, establishing priorities, activating or expanding the Incident Command Structure, approving major protective or operational actions, and briefing executive leadership. This position maintains command at Sun Peak Energy's Emergency Operations Center and ensures decisions are coordinated across safety, operations, information technology, communications, planning, logistics, liaison, and finance functions.

Role Focus During Exercise: Establish incident objectives, determine escalation thresholds, decide whether additional ICS positions are needed, balance restoration with safety and cybersecurity concerns, manage executive expectations, and determine when response conditions require protective actions such as access restrictions, forensic procedures, shelter-in-place, evacuation, demobilization, or transition to recovery. Chair of the Incident Command team.

Sun Peak Energy Context:

- Mid-sized Orange County electric utility serving residential, commercial, municipal, tourism, and high-visibility customers.
- Key customers and venues include Disneyland Resort, Anaheim Convention Center, Honda Center, Angel Stadium, state beaches, and dense residential areas.
- Disruptions may quickly involve customer confidence, public safety concerns, elected official interest, executive attention, and regional economic impacts.
- The team has not been through an emergency exercise in years, and emergency plans have not been reviewed or updated meaningfully in a long time. The Incident Command Team is not practiced working together in this environment.



SAFETY OFFICER

Position Parameters: The Safety Officer monitors incident conditions for hazards to employees, field crews, customer-facing staff, contractors, visitors, and the public. This position advises the Incident Commander on protective measures, evaluates risks created by power fluctuations, extended work shifts, restricted access, shelter-in-place, evacuation, workplace violence concerns, and public frustration, and helps ensure response actions do not create unnecessary harm.

Role Focus During Exercise: Identify immediate and emerging hazards, recommend protective actions for staff and facilities, support workplace violence response considerations, coordinate with Operations and Logistics on safe staffing and site controls, and ensure employee safety remains a priority while the organization restores service and investigates the cyber-related disruption.

Sun Peak Energy Context:

- Sun Peak Energy has approximately 1,200 employees across office, field, customer service, engineering, IT, cybersecurity, emergency management, safety, finance, and leadership functions.
- Normal shifts typically end around 5:00 p.m.
- On-call and extended staffing may be needed during incidents.
- The Safety Officer should account for fatigue, employee anxiety, field hazards, and potential employee assistance needs.

PUBLIC INFORMATION OFFICER

Position Parameters: The Public Information Officer develops, coordinates, and releases approved information for employees, customers, media, community partners, elected officials, and other external audiences. This position ensures messaging is accurate, timely, consistent, and appropriately cautious when facts are incomplete, especially when power disruptions, online account access issues, service interruptions, cyber concerns, or social media activity generate public attention.

Role Focus During Exercise: Prepare internal and external talking points, coordinate with the Incident Commander before releasing information, manage media and social media inquiries, support employee communications, identify what should and should not be shared publicly, and maintain a calm, transparent tone that acknowledges impacts without speculating on causes or technical details.

Sun Peak Energy Context:

- Sun Peak Energy serves communities and high-profile venues across Orange County.
- Communications may quickly reach customers, tourism partners, municipal stakeholders, media outlets, and elected officials.
- Customers may experience power loss, power surges, difficulty accessing online accounts, and inability to call the facility if VOIP systems are down.
- Public concern may focus on the reliability of electric service.

LIAISON OFFICER

Position Parameters: The Liaison Officer coordinates with external agencies, utilities, public safety partners, government representatives, critical customers, mutual aid contacts, industry information-sharing organizations, and other stakeholders. This position helps the Incident Commander understand outside concerns, requests, available support, and coordination needs without overloading command or operations with separate stakeholder conversations.

Role Focus During Exercise: Identify who needs to be contacted, establish stakeholder coordination priorities, support information sharing with external partners, clarify whether neighboring utilities are affected, coordinate law enforcement support if a workplace violence threat emerges, and help manage elected official and critical customer expectations in coordination with the Public Information Officer.

Sun Peak Energy Context:

- Sun Peak Energy's service area includes municipalities, high-visibility entertainment and sports venues, coastal communities, and essential service providers.
- The Liaison Officer may need to coordinate with neighboring utilities, local emergency management, law enforcement, elected officials' offices, CISA or industry cybersecurity partners, major customers, and other infrastructure providers.
- External stakeholders may request situational awareness or support during the disruption.

OPERATIONS SECTION CHIEF

Position Parameters: The Operations Section Chief directs tactical response activities needed to stabilize the incident, maintain or restore electric service, support field operations, manage operational staffing, and implement Incident Commander priorities. This position coordinates field crews, outage response, system monitoring, service restoration, site access controls, and operational impacts caused by physical or digital restrictions.

Role Focus During Exercise: Determine available operational resources, manage staff nearing the end of shift, coordinate field and control activities, assess whether mutual aid or neighboring utility support is needed, implement access or site restrictions if ordered, support restoration priorities, and provide the Incident Commander with realistic operational options and constraints.

Sun Peak Energy Context:

- Sun Peak Energy provides electric distribution, customer support, outage response, field operations, and grid monitoring services across most of Orange County.
- Field teams initially report no physical infrastructure issues.
- The disruption may involve digital systems, operational technology, or system monitoring rather than traditional equipment failure.
- Normal shift changes around 5:00 p.m. may affect staffing continuity.
- A business continuity plan exists, but it has not been meaningfully reviewed or updated in over 5 years. There is little confidence in the plan.

INFORMATION TECHNOLOGY UNIT LEADER

Position Parameters: The Information Technology Unit Leader provides technical leadership for information technology, cybersecurity, network access, identity and credential concerns, forensic coordination, digital containment, system restoration, and communications technology issues. This position advises command on risks and tradeoffs related to shutting down digital access, isolating systems, preserving evidence, maintaining operational continuity, and restoring service safely.

Role Focus During Exercise: Assess cyber indicators, determine whether additional technical resources are needed, recommend containment or access restrictions, coordinate forensic procedures, confirm credential revocation risks, advise on impacts to VOIP, VPN, monitoring, and remote access, support safe system restart, and explain technical findings in plain language so command can make informed decisions.

Sun Peak Energy Context:

- Sun Peak Energy relies on customer-facing systems, internal business platforms, field communications, operational technology, monitoring infrastructure, VOIP phones, and remote access tools.
- The exercise includes unusual outbound traffic from a network segment connected to operational systems.
- Indicators include repeated authentication attempts, data transfer to unfamiliar external IP addresses, and potential credential compromise.
- Later concerns include an adversary emulation exercise affecting real-world systems.
- An Information Technology Disaster Recovery Plan exists, but it has not been meaningfully reviewed or updated in 3+ years and there is little confidence in the plan.
- Recent testing and exercises have been initiated on the digital infrastructure.

PLANNING SECTION CHIEF

Position Parameters: The Planning Section Chief supports incident management by collecting information, maintaining situational awareness, anticipating future conditions, developing response objectives, preparing or coordinating an Incident Action Plan when needed, documenting key decisions, tracking assumptions, and identifying recovery or after-action issues. This position helps the team think beyond the immediate problem and plan for prolonged operations.

Role Focus During Exercise: Track what is known and unknown, identify planning assumptions, recommend whether an Incident Action Plan is needed, document key decisions and incident timelines, anticipate outcomes of access shutdowns or evacuations, plan for staffing past 5:00 p.m., capture improvement opportunities, and support transition from response to recovery and demobilization.

Sun Peak Energy Context:

- The incident may begin as scattered customer complaints.
- The situation may evolve into cyber containment, physical access restrictions, public communications, workplace violence concerns, extended staffing, restoration sequencing, and executive or elected official involvement.
- The service area includes high-visibility venues and residential communities.
- Planning should account for cascading operational, reputational, staffing, and public safety implications.

LOGISTICS SECTION CHIEF

Position Parameters: The Logistics Section Chief obtains and supports the resources, services, equipment, facilities, communications, supplies, transportation, food, workspace, and contractor support needed for the incident response. This position ensures responders can continue working safely and effectively, especially if access restrictions, extended operations, digital outages, or facility limitations create resource gaps.

Role Focus During Exercise: Identify what people need to continue response operations, obtain equipment not connected to the affected network, support alternate communications, manage deliveries or staging if access is restricted, coordinate food and basic needs for extended staffing, activate or stand down vendors and contracts, and ensure resource requests are documented and prioritized.

Sun Peak Energy Context:

- Sun Peak Energy operates from a primary office and Emergency Operations Center west of Anaheim.
- The company maintains field operations yards and service staging areas across Orange County.
- The incident may require alternate communications if VOIP phones fail.
- IT or forensic work may require non-networked equipment.
- Staff support may be needed during shelter-in-place or extended shifts.
- Delivery coordination may be needed if physical access is restricted.
- Contractor or vendor support may be needed for technical response.

ADMIN/FINANCE SECTION CHIEF

Position Parameters: The Admin/Finance Section Chief tracks costs, contracts, labor, timekeeping, procurement, claims, administrative requirements, and business impacts related to the incident. This position supports command by identifying financial consequences, documenting emergency expenses, managing overtime considerations, supporting labor pool decisions, and coordinating administrative needs for extended or unusual operations.

Role Focus During Exercise: Track incident-related costs, determine emergency budget availability, support overtime and labor pool decisions, coordinate procurement and contracting needs, document administrative decisions, support employee assistance considerations, manage drawdown costs, and help preserve records that may be needed for reimbursement, audit, legal review, or after-action improvement planning.

Sun Peak Energy Context:

- Sun Peak Energy's normal office and field shifts typically end around 5:00 p.m.
- An incident extending into the evening may trigger overtime, staffing, contractor, labor relations, and cost tracking considerations.
- The scenario includes a recently terminated cybersecurity analyst with elevated privileges.
- Coordination with human resources, legal, cybersecurity, and leadership may be important for access review and administrative documentation.